UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 9,953,149 B2
APPLICATION NO. : 14/839505
DATED : April 24, 2018
INVENTOR(S) : Kevin Alan Tussy

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Claims

Claim 4, Lines 58 through 59:
"imaging of the at least on second image; and"
Should read:
--imaging of the at least one second image; and--

Signed and Sealed this
Fourth Day of September, 2018

Andrei Iancu
Director of the United States Patent and Trademark Office

FACETEC EXHIBIT 2013
JUMIO v. FACETEC
IPR2025-00108

PTO/SB/44 (09-07)
Approved for use through 01/31/2020. OMB 0651-0033
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.
(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 9,953,149

APPLICATION NO.: 14/839,505

ISSUE DATE : April 24, 2018

INVENTOR(S) : Kevin Alan Tussy

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Page 37, Claim 4, Column Lines 58 through 59, "imaging of the at least on second image; and" should read:

--imaging of the at least one second image; and--

MAILING ADDRESS OF SENDER (Please do not use Customer Number below):
Chad W. Miller
Weide & Miller, Ltd.
10655 Park Run Drive, Suite 100
Las Vegas, NV 89144

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1.0 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Attention Certificate of Corrections Branch, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt	
EFS ID:	33423899
Application Number:	14839505
International Application Number:	
Confirmation Number:	6236
Title of Invention:	Facial Recognition Authentication System Including Path Parameters
First Named Inventor/Applicant Name:	Kevin Alan Tussy
Customer Number:	32856
Filer:	Chad W. Miller
Filer Authorized By:	
Attorney Docket Number:	FACIAL.0012P
Receipt Date:	09-AUG-2018
Filing Date:	28-AUG-2015
Time Stamp:	15:49:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	CWMW13165REQCERTCORR.pdf	17944 ac947b19c52bb4022840e3490954663099f416fe	no	1

Warnings:

Information:					
2	Request for Certificate of Correction	FACIAL0012PCERTOFCORRSB44.pdf	89196 70f46b6a3cf8add44afb9112c58eea054596604e	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	107140	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	FaceTec, Inc
Patent No.	:	9,953,149
Issued	:	April 24, 2018
Appl. No.	:	14/839,505
Filed	:	August 28, 2015
For	:	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Patent Office via EFSWeb filing, on:

August 9, 2018
(Date)

/Chad W. Miller/
Chad W. Miller Reg. No. 44,943

REQUEST FOR CERTIFICATE OF CORRECTION

Attn: Certificate of Corrections Branch
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Enclosed for filing is a Certificate of Correction with respect to the above-referenced patent. The error which is cited in the Certificate of Correction, was incurred through a mistake on the part of the U.S. Patent and Trademark Office, and therefore a fee is not required in accordance with 37 C.F.R. Section 1.322. Applicant respectfully submits that this mistake does not involve changes that would constitute new matter or require reexamination of the patent.

Respectfully submitted,

Dated: August 9, 2018

By: /Chad W. Miller/
Chad W. Miller
Attorney of Record
Registration No. 44,943
Weide & Miller, Ltd.
10655 Park Run Drive, Suite 100
Las Vegas, NV 89144
(702) 382-4804 (Pacific Time)
cmiller@weidemiller.com

CWM-W-13165

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/839,505	04/24/2018	9953149	FACIAL.0012P	6236

32856 7590 04/04/2018

WEIDE & MILLER, LTD.
10655 Park Run Drive
SUITE 100
LAS VEGAS, NV 89144

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 201 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Kevin Alan Tussy, Las Vegas, NV;
FACETEC, INC., Las Vegas, NV;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/839,505	08/28/2015	Kevin Alan Tussy	FACIAL.0012P

CONFIRMATION NO. 6236

32856
WEIDE & MILLER, LTD.
10655 Park Run Drive
SUITE 100
LAS VEGAS, NV 89144

PUB REQUEST ACCEPTANCE LETTER

OC000000098243317

Date Mailed: 03/22/2018

NOTICE OF ACCEPTANCE OF PUBLICATION REQUEST

The request for voluntary publication, amended publication, early publication, redacted publication, republication, corrected publication or revised publication has been received for this application. The request, including payment of any necessary fee(s), is in compliance with 37 CFR 1.215, 1.217, 1.219 or 1.221.

The projected publication date is 06/28/2018.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/npfarmer/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2003/0236832	12/03	McIntyre, et al.			
		6,678,664	01/04	Ganesan			
		6,687,390	02/04	Avni			
		6,697,502	02/04	Luo			
		6,728,401	04/04	Hardeberg			
		2004/0070678	04/04	Toyama, et al.			
		2004/0081338	04/04	Takenaka			
		2004/0125991	07/04	Yokoi			
		2004/0143598	07/04	Drucker, et al.			
		6,775,397	08/04	Hamalainen			
		2004/0190758	09/04	Doi, et al.			
		2004/0109584	10/04	Lestideau			
		2004/0201709	10/04	McIntyre, et al.			
		6,840,149	01-2005 ~~10/04~~	~~Squilla, et al.~~ Beal			
Change(s) applied to document, /C.M./ 12/27/2017		~~20047/0264780~~	~~12/04~~	~~Zhang, et al.~~			
		2005/0031173	02/05	Hwang			
		2005/0065855	03/05	Geller			
		2005/0094849	05/05	Sung, et al.			
		2005/0100195	05/05	Li			
		2005/0117802	06/05	Yonaha, et al.			
		2005/0141766	06/05	Nagahashi, et al.			
		2005/0180627	08/05	Yang, et al.			
		2005/0190273	09/05	Toyama, et al.			
		2005/0220347	10/05	Enomoto			
		2005/0251015	11/05	Takikawa, et al.			
		2005/0265603	12/05	Porter, et al.			

EXAMINER	/SHANTO ABEDIN/	DATE CONSIDERED	12/22/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		5,031,228	07/91	Lu			
		5,699,449	12/97	Javidi			
		5,784,056	07/98	Nielsen			
		5,835,616	11/98	Lobo, et al.			
		6,212,030	~~07/91~~ 04-2001	~~Lu~~ Koriyama et al.			
Change(s) applied to document, /C.M/ 12/27/2017		6,461,807	~~12/97~~ 10-2002	~~Javidi~~ Friend et al.			
		6,961,361	~~11/98~~ 11-2005	~~Lobo, et al.~~ Tanaka			
		7,211,138	~~07/91~~ 05-2007	~~Lu~~ Yamamoto et al.			
		7,460,916	~~12/97~~ 12-2008	~~Javidi~~ Batruni			
		7,710,693	~~07/98~~ 05-2010	~~Nielsen~~ Guzman-Casillas et al.			
		7,960,470	~~11/98~~ 06-2011	~~Lobo, et al.~~ Okahira			
		8,210,247	~~07/91~~ 07-2012	~~Lu~~ Blomgren			
		8,460,024	~~12/97~~ 06-2013	~~Javidi~~ Damodharan et al.			
		8,709,801	~~07/98~~ 04-2014	~~Nielsen~~ Pan et al.			
		8,959,578	~~11/98~~ 02-2015	~~Lobo, et al.~~ Simpson et al.			
		9,209,355	~~07/91~~ 12-2015	~~Lu~~ Senda et al.			
		9,459,132	~~12/97~~ 10-2016	~~Javidi~~ Fehrenbach et al.			
		9,708,909	~~07/98~~ 07-2017	~~Nielsen~~ Atkinson et al.			
		9,958,687	11/98	Lobo, et al.			
		~~10,208,464~~	~~07/91~~	~~Lu~~			
		~~10,458,241~~	~~12/97~~	~~Javidi~~			
		~~10,957,795~~	~~11/98~~	~~Lobo, et al.~~			
		~~11,207,572~~	~~07/91~~	~~Lu~~			
		~~11,457,349~~	~~12/97~~	~~Javidi~~			
		5,031,228	07/91	Lu			
		5,699,449	12/97	Javidi			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/22/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

Office of Petitions: Routing Sheet

Application No. 14839505

This application is being forwarded to your office for further processing. A decision has been rendered on a petition filed in this application, as indicated below. For details of this decision, please see the document PET.OP.DEC filed on the same date as this document.

- [X] **GRANTED**
- [ ] **DISMISSED**
- [ ] **DENIED**

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/839,505	08/28/2015	Kevin Alan Tussy	FACIAL.0012P	6236

32856 7590 03/19/2018

WEIDE & MILLER, LTD.
10655 Park Run Drive
SUITE 100
LAS VEGAS, NV 89144

EXAMINER	
ABEDIN, SHANTO	

ART UNIT	PAPER NUMBER
2494	

MAIL DATE	DELIVERY MODE
03/19/2018	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

In re Application of	:	
Kevin Alan Tussy	:	
Application No. 14/839,505	:	DECISION ON PETITION
Filed: August 28, 2015	:	
Attorney Docket No. FACIAL.0012P	:	

This is a decision on the petition under 37 CFR 1.78(c) filed February 23, 2018, requesting acceptance of unintentionally delayed claims under 35 U.S.C. 119(e) for the benefit of prior-filed provisional applications as set forth in the accompanying Corrected ADS Form.

The petition is **GRANTED.**

If the reference required by 35 U.S.C. 119(e) and 37 CFR 1.78(a)(3) is presented after the time period provided by 37 CFR 1.78(a)(4), the claim under 35 U.S.C. 119(e) for the benefit of a prior-filed provisional application may be accepted if the reference required by 37 CFR 1.78(a)(3) was unintentionally delayed. A petition to accept an unintentionally delayed claim under 35 U.S.C. 119(e) for the benefit of prior-filed provisional application must be accompanied by:

(1) The reference required by 35 U.S.C. 119(e) and 37 CFR 1.78(a)(3) to the prior-filed application, unless previously submitted. The reference must be included in an application data sheet (§ 1.76(b)(5));

(2) The petition fee as set forth in § 1.17(m); and

(3) A statement that the entire delay between the date the benefit claim was due under 37 CFR 1.78(a)(4) and the date the benefit claim was filed was unintentional. The Director may require additional information where there is a question whether the delay was unintentional.

As the present petition satisfies all the above requirements, the claims under 35 U.S.C. 119(e) for the benefit of the prior-filed applications are accepted as being unintentionally delayed.

Applicant is advised that this decision grants the petition to accept the unintentionally delayed domestic benefit claims to the prior-filed applications because the petition requirements of 37 CFR 1.78(c) and the formal requirements for claiming domestic benefit (see MPEP 211.01 et. seq.) have been met. This acceptance should not be construed as meaning that this application is entitled to the benefit of the prior-filed applications. Whether a claimed invention in a

nonprovisional application is entitled to the benefit of the filing date of a prior-filed application on the basis of the disclosure thereof is determined during examination if it becomes necessary to do so (e.g., intervening reference and interference proceeding). See MPEP 211.05.

A corrected Filing Receipt, which includes the claims for the benefit of the prior-filed applications, accompanies this decision on petition.

This application is being forwarded to the Office of Data Management.

Any questions concerning this matter may be directed to the undersigned at (571) 272-3211.

/Christina Tartera Donnell/

Christina Tartera Donnell
Attorney Advisor
Office of Petitions

Enclosure: Corrected Filing Receipt

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/839,505	08/28/2015	2494	770	FACIAL.0012P	21	3

CONFIRMATION NO. 6236

CORRECTED FILING RECEIPT

32856
WEIDE & MILLER, LTD.
10655 Park Run Drive
SUITE 100
LAS VEGAS, NV 89144

Date Mailed: 03/16/2018

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Kevin Alan Tussy, Las Vegas, NV;

Applicant(s)

FACETEC, INC., Las Vegas, NV;

Power of Attorney: The patent practitioners associated with Customer Number 000032856

Domestic Priority data as claimed by applicant

This appln claims benefit of 62/043,224 08/28/2014
and claims benefit of 62/054,847 09/24/2014
and claims benefit of 62/064,415 10/15/2014
and claims benefit of 62/085,963 12/01/2014
and claims benefit of 62/101,317 01/08/2015
and claims benefit of 62/139,558 03/27/2015
and claims benefit of 62/188,584 07/03/2015

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: No

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 09/11/2015

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/839,505**

Projected Publication Date: Not Applicable

Non-Publication Request: No

Early Publication Request: No
** SMALL ENTITY **
Title

Facial Recognition Authentication System Including Path Parameters

Preliminary Class

726

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

Office of Petitions: Decision Count Sheet

Mailing Month 3

Application No. 14839505

14839505

For US serial numbers: enter number only, no slashes or commas. Ex: 10123456
For PCT: enter "51+single digit of year of filing+last 5 numbers", Ex. for PCT/US05/12345, enter 51512345

Deciding Official: Christina Donnell

Count (1) - Palm Credit 14839505

Decision: GRANT

FINANCE WORK NEEDED
☐ Select Check Box for YES

GRANT

Decision Type: 535 - 37 CFR 1.78(a)(3) & (a)(6) UNINTENTIONAL DELAY

535

Notes:

Count (2)

Decision: n/a

FINANCE WORK NEEDED
☐ Select Check Box for YES

Decision Type: NONE

Notes:

Count (3)

Decision: n/a

FINANCE WORK NEEDED
☐ Select Check Box for YES

Decision Type: NONE

Notes:

Initials of Approving Official (if required)

If more than 3 decisions, attach 2nd count sheet & mark this box ☐

Printed on: 3/15/2018

Office of Petitions Internal Document - Ver. 5.0

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/839,505	08/28/2015	2494	770	FACIAL.0012P	21	3

CONFIRMATION NO. 6236

CORRECTED FILING RECEIPT

32856
WEIDE & MILLER, LTD.
10655 Park Run Drive
SUITE 100
LAS VEGAS, NV 89144

OC000000098115057

Date Mailed: 03/16/2018

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Kevin Alan Tussy, Las Vegas, NV;

Applicant(s)

FACETEC, INC., Las Vegas, NV;

Power of Attorney: The patent practitioners associated with Customer Number 000032856

Domestic Priority data as claimed by applicant

This appln claims benefit of 62/043,224 08/28/2014
and claims benefit of 62/054,847 09/24/2014
and claims benefit of 62/064,415 10/15/2014
and claims benefit of 62/085,963 12/01/2014
and claims benefit of 62/101,317 01/08/2015
and claims benefit of 62/139,558 03/27/2015
and claims benefit of 62/188,584 07/03/2015

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: No

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 09/11/2015

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/839,505**

Projected Publication Date: Not Applicable

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****
Title

Facial Recognition Authentication System Including Path Parameters

Preliminary Class

726

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

32856 7590 12/15/2017
WEIDE & MILLER, LTD.
10655 Park Run Drive
SUITE 100
LAS VEGAS, NV 89144

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Brian G. Prince	(Depositor's name)
March 15, 2018	(Signature)
/Brian G. Prince/	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/839,505	08/28/2015	Kevin Alan Tussy	FACIAL.0012P	6236

TITLE OF INVENTION: Facial Recognition Authentication System Including Path Parameters

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	03/15/2018

EXAMINER	ART UNIT	CLASS-SUBCLASS
ABEDIN, SHANTO	2436	726-006000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Weide & Miller, Ltd.
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: FaceTec, Inc.
(B) RESIDENCE: (CITY and STATE OR COUNTRY): Las Vegas, NV

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
☒ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☒ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 502200 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
☐ Applicant certifying micro entity status. See 37 CFR 1.29
NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
☐ Applicant asserting small entity status. See 37 CFR 1.27
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
☐ Applicant changing to regular undiscounted fee status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature Brian G. Prince Date /Brian G. Prince/
Typed or printed name March 15, 2018 Registration No. 70,569

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Electronic Patent Application Fee Transmittal

Application Number:	14839505
Filing Date:	28-Aug-2015
Title of Invention:	Facial Recognition Authentication System Including Path Parameters
First Named Inventor/Applicant Name:	Kevin Alan Tussy
Filer:	Brian G. Prince
Attorney Docket Number:	FACIAL.0012P

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	2501	1	480	480

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**480**

Electronic Acknowledgement Receipt	
EFS ID:	32069308
Application Number:	14839505
International Application Number:	
Confirmation Number:	6236
Title of Invention:	Facial Recognition Authentication System Including Path Parameters
First Named Inventor/Applicant Name:	Kevin Alan Tussy
Customer Number:	32856
Filer:	Brian G. Prince
Filer Authorized By:	
Attorney Docket Number:	FACIAL.0012P
Receipt Date:	15-MAR-2018
Filing Date:	28-AUG-2015
Time Stamp:	18:42:20
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$480
RAM confirmation Number	031618INTEFSW18431000
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	FACIAL0012PISSUEFEEPDF.pdf	147163 67054b59980ab299ad34b39af8463450011 7a1d6	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30127 60a2ac32873a9624ef5618218426b1b329a b1160	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	177290		

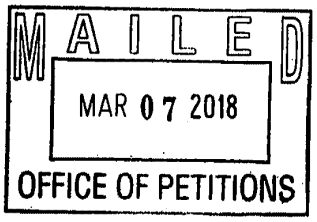
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

WEIDE & MILLER, LTD.
10655 Park Run Drive
SUITE 100
LAS VEGAS NV 89144



In re Application of	:	
Kevin Alan Tussy	:	
Application No. 14/839,505	:	DECISION DISMISSING PETITION
Filed: August 28, 2015	:	UNDER 37 CFR 1.313(a)
Attorney Docket No. **FACIAL.0012P**	:	

This is a decision on the petition under 37 CFR 1.313(a), filed February 23, 2018, requesting withdrawal of the above-identified application from issue.

The petition is **dismissed** as moot for the reasons stated below.

A review of the file record discloses that a Notice of Allowance and Fee(s) Due was mailed on December 15, 2017, with the issue fee being due on or before March 15, 2018. The petition states that the issue fee in this case has not been paid.

The filing of a petition under 37 CFR 1.313(a) is unnecessary, since the mere filing of an RCE and submission will effectively withdraw an application from issue prior to payment of the issue fee. In view thereof, the petition to withdraw from issue is dismissed as involving a moot issue. *Note* MPEP §§ 706.07(h)(IX) and 1308.

Inquiries concerning this decision may be directed to Terri at (571) 272-2991.

/Terri Johnson/
Terri Johnson
Paralegal Specialist
Office of Petitions

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/839,505	08/28/2015	Kevin Alan Tussy	FACIAL.0012P

CONFIRMATION NO. 6236

32856
WEIDE & MILLER, LTD.
10655 Park Run Drive
SUITE 100
LAS VEGAS, NV 89144

POA ACCEPTANCE LETTER

OC000000097676441

Date Mailed: 02/27/2018

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/23/2018.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/ttran/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/839,505	08/28/2015	2494	770	FACIAL.0012P	21	3

CONFIRMATION NO. 6236

CORRECTED FILING RECEIPT

32856
WEIDE & MILLER, LTD.
10655 Park Run Drive
SUITE 100
LAS VEGAS, NV 89144

OC000000097678498

Date Mailed: 02/27/2018

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Kevin Alan Tussy, Las Vegas, NV;

Applicant(s)

FACETEC, INC., Las Vegas, NV;

Power of Attorney: The patent practitioners associated with Customer Number 000032856

Domestic Priority data as claimed by applicant

This appln claims benefit of 62/043,224 08/28/2014

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: No

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 09/11/2015
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/839,505**
Projected Publication Date: Not Applicable

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****
Title

Facial Recognition Authentication System Including Path Parameters

Preliminary Class

726

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor	:	Kevin Alan Tussy
Application No.:		14/839,505
Filing Date	:	August 28, 2015
For	:	Facial Recognition Authentication System Including Path Parameters
Examiner	:	ABEDIN, SHANTO

Group Art Unit: 2494

I hereby certify that this document is being transmitted electronically to the United States Patent and Trademark Office via the EFS Web e- Filing system on:

February 23, 2018
(Date)

/Brian G. Prince/
Brian G. Prince, Reg. # 70,569

PETITION FOR ACCEPTANCE OF AN UNINTENTIONALLY DELAYED PRIORITY CLAIM UNDER 37 C.F.R. § 1.78 (c)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The Applicant hereby petitions for acceptance of an unintentionally delayed priority claim under 37 C.F.R. § 1.78(c). In accordance with Section 1.78(c):

1) The Applicant has included a corrected ADS herewith which references the prior-filed provisional applications in accordance with 35 U.S.C. § 119(e) and 1.78(a)(3);

2) The Applicant has submitted herewith the fee under 1.17(m); and

3) The Applicant states that the entire delay between the date the benefit claim was due under paragraph (a)(4) of Section 1.78 and the date of the filing of this benefit claim herein, was unintentional.

Respectfully submitted,

Date: February 23, 2018

/Brian G. Prince/

Brian G. Prince
Registration No. 70,569
Weide & Miller, Ltd.
10655 Park Run Dr. Suite 100
Las Vegas, NV 89144
bprince@weidemiller.com
(702) 382-4804 (Pacific Time)

The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Account No.: 502200.

FACIAL.0012P PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor	:	Kevin Alan Tussy
Application No.:		14/839,505
Filing Date	:	August 28, 2015
For	:	Facial Recognition Authentication System Including Path Parameters
Examiner	:	ABEDIN, SHANTO

Group Art Unit: 2494

I hereby certify that this document is being transmitted electronically to the United States Patent and Trademark Office via the EFS Web e- Filing system on:

February 23, 2018
(Date)

/Brian G. Prince/
Brian G. Prince, Reg. # 70,569

PETITION TO WITHDRAW FROM ISSUE UNDER 37 § C.F.R. 1.313(a)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The Applicant hereby requests that the above-mentioned application be withdrawn from issue under 37 C.F.R. § 1.313(a). This petition is being filed prior to payment of the issue fee. The petition fee set forth under 37 C.F.R. § 1.17(h) is also provided herewith.

The Application should be withdrawn to allow for the consideration and resolution of the Applicant's Petition for Acceptance of an Unintentionally Delayed Priority Claim Under 37 C.F.R. § 1.78(c) which is also filed herewith. It is respectfully submitted that this reason is sufficient under 37 C.F.R. § 1.131(a).

Respectfully submitted,

Date: February 23, 2018

/Brian G. Prince/

Brian G. Prince
Registration No. 70,569
Weide & Miller, Ltd.
10655 Park Run Drive Suite 100
Las Vegas, NV 89144
bprince@weidemiller.com
(702) 382-4804 (Pacific Time)

The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Account No.: 502200.

Electronic Patent Application Fee Transmittal	
Application Number:	14839505
Filing Date:	28-Aug-2015
Title of Invention:	Facial Recognition Authentication System Including Path Parameters
First Named Inventor/Applicant Name:	
Filer:	Brian G. Prince
Attorney Docket Number:	FACIAL.0012P

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
PROCESSING FEE, EXCEPT PROV. APPLS.	2830	1	70	70
PET. DELAY SUB OR RESTORE PRIORITY-CLAIM	2454	1	1000	1000
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1070**

Electronic Acknowledgement Receipt	
EFS ID:	31878077
Application Number:	14839505
International Application Number:	
Confirmation Number:	6236
Title of Invention:	Facial Recognition Authentication System Including Path Parameters
First Named Inventor/Applicant Name:	
Customer Number:	32856
Filer:	Brian G. Prince
Filer Authorized By:	
Attorney Docket Number:	FACIAL.0012P
Receipt Date:	23-FEB-2018
Filing Date:	28-AUG-2015
Time Stamp:	20:10:50
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1070
RAM confirmation Number	022618INTEFSW20104800
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet to update/ correct info	CorrectedADS.pdf	100856 4f602d9b17f98e04d818a9581dcb9bda4610ccc2	no	7
Warnings:					
Information:					
2	Assignee showing of ownership per 37 CFR 3.73	FACIAL0012P373STMNTPDF.pdf	66380 a7c21f82a74c8a045621039d6010c5a7b4c71d1d	no	2
Warnings:					
Information:					
3	Petition for review by the Office of Petitions	BGPW2031PETITION.pdf	17787 56d80a77aabd8e8dbff9be0313426877c940999c	no	1
Warnings:					
Information:					
4	Petition for review by the Office of Petitions	BGP-W-2045-PetitionToWithdrawFromIssue.pdf	17701 585b862e4646501aa5bc5adb77abb5f7022d6dab	no	1
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	31911 4aab7814589c61ba604c2cc92857af9b25c7083a	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	234635		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Document Description: Application Data Sheet to update/correct info
Doc Code: ADS.CORR

CORRECTED ADS FORM

Application Number	14839505
Title of Invention	Facial Recognition Authentication System Including Path Parameters

Inventor Information

****If no data is shown, no data has been corrected****

	Data of Record	Updated Data
Order Number		
Name		
Residence Information		
Residency		
City		
State		
Country of Residence		
Mailing Address of Inventor		
Address 1		
Address 2		
City,State/Province, Postal Code		
Country		

Document Description: Application Data Sheet to update/correct info
Doc Code: ADS.CORR

Application Information

	Data of Record	Updated Data
Title of Invention	Facial Recognition Authentication System Including Path Parameters	
Attorney Docket Number	FACIAL.0012P	
Entity Type	Small	

Domestic Benefit/National Stage Information

****If no data is shown, no data has been corrected****

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121,365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S. C. 119(e) or 120, and 37 CFR 1.78(a).

		Data of Record	Updated Data
	Prior Application Status	pending	
	Application Number	14839505	
	Continuity Type	PRO	
	Prior Application Number	62043224	
	Filing Date (YYYY-MM-DD)	2014-08-28	
	Patent Number		
	Issue Date (YYYY-MM-DD)	0001-01-01	

		Data of Record	Updated Data
	Prior Application Status		expired
	Application Number		14839505
	Continuity Type		PRO
	Prior Application Number		62054847
	Filing Date (YYYY-MM-DD)		2014-09-24
	Patent Number		
	Issue Date (YYYY-MM-DD)		

		Data of Record	Updated Data
	Prior Application Status		expired
	Application Number		14839505
	Continuity Type		PRO
	Prior Application Number		62064415
	Filing Date (YYYY-MM-DD)		2014-10-15
	Patent Number		
	Issue Date (YYYY-MM-DD)		

		Data of Record	Updated Data
	Prior Application Status		expired
	Application Number		14839505
	Continuity Type		PRO
	Prior Application Number		62085963
	Filing Date (YYYY-MM-DD)		2014-12-01
	Patent Number		
	Issue Date (YYYY-MM-DD)		

		Data of Record	Updated Data
	Prior Application Status		expired
	Application Number		14839505
	Continuity Type		PRO
	Prior Application Number		62101317
	Filing Date (YYYY-MM-DD)		2015-01-08
	Patent Number		
	Issue Date (YYYY-MM-DD)		

		Data of Record	Updated Data
	Prior Application Status		expired
	Application Number		14839505
	Continuity Type		PRO
	Prior Application Number		62139558
	Filing Date (YYYY-MM-DD)		2015-03-27
	Patent Number		
	Issue Date (YYYY-MM-DD)		

		Data of Record	Updated Data
	Prior Application Status		expired
	Application Number		14839505
	Continuity Type		PRO
	Prior Application Number		62188584
	Filing Date (YYYY-MM-DD)		2015-07-03
	Patent Number		
	Issue Date (YYYY-MM-DD)		

Document Description: Application Data Sheet to update/correct info
Doc Code: ADS.CORR

Foreign Priority Information

****If no data is shown, no data has been corrected****

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

		Data of Record	Updated Data
	Application Number		
	Country		
	Filing Date		
	Access Code		

Applicant Information

****If no data is shown, no data has been corrected****
Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

	Data of Record	Updated Data
Applicant Type		ASG
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is		
Name of the Deceased or Legally Incapacitated Inventor		
Applicant is an Organization		Yes
Name		
Organization Name		FACETEC, INC.
Address 1		1707 Village Center Circle, Suite 200

Corrected ADS 1.0

Address 2		
City,State/Province,Postal Code		Las Vegas NV 89134
Country		US
Phone Number		
Fax Number		
Email Address		

Assignee Information including Non-Applicant Assignee Information

****If no data is shown, no data has been corrected****
Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office

	Data of Record	Updated Data
Order		
Applicant is an Organization		
Name		
Organization Name		

Mailing Address

Address 1		
Address 2		
City,State/Province,Postal Code		
Country		
Phone Number		
Fax Number		

Email Address		

Signature

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b).

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Brian G. Prince/	Registration Number	70569
First Name	Brian	Last Name	Prince

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: Kevin Alan Tussy

Application No./Patent No.: 14/839,505 Filed/Issue Date: August 28, 2015

Titled: Facial Recognition Authentication System Including Path Parameters

FaceTec, Inc., a corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☑ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 038869, Frame 0813, or for which a copy thereof is attached.

B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

   1. From: _____ To: _____

      The document was recorded in the United States Patent and Trademark Office at

      Reel _____, Frame _____, or for which a copy thereof is attached.

   2. From: _____ To: _____

      The document was recorded in the United States Patent and Trademark Office at

      Reel _____, Frame _____, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☑ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Brian G. Prince/	February 23, 2018
Signature	Date
Brian G. Prince	70,569
Printed or Typed Name	Title or Registration Number

[Page 2 of 2]

PTO/AIA/82A (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	14/839,505
Filing Date	August 28, 2015
First Named Inventor	Kevin Alan Tussy
Title	Facial Recognition Authentication System Including Path Parameters
Art Unit	2494
Examiner Name	Shanto Abedin
Attorney Docket Number	FACIAL.0012P

SIGNATURE of Applicant or Patent Practitioner

Signature	/Brian G. Prince/	Date (Optional)	
Name	Brian G. Prince	Registration Number	70569
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ *Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 000032856

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

FACETEC, INC.

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature		Date (Optional)	
Name	Kevin Alan Tussy		
Title	President for FaceTec, Inc.		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt	
EFS ID:	31878119
Application Number:	14839505
International Application Number:	
Confirmation Number:	6236
Title of Invention:	Facial Recognition Authentication System Including Path Parameters
First Named Inventor/Applicant Name:	Kevin Alan Tussy
Customer Number:	32856
Filer:	Brian G. Prince
Filer Authorized By:	
Attorney Docket Number:	FACIAL.0012P
Receipt Date:	23-FEB-2018
Filing Date:	28-AUG-2015
Time Stamp:	20:12:31
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	FACETC0012PPOA.pdf	231567 154ee0a7506d04c506b0b4a6cd37fab5bc30c5bc	no	2

Warnings:

Information:	
Total Files Size (in bytes):	231567

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		5,031,228	07/91	Lu			
		5,699,449	12/97	Javidi			
		5,784,056	07/98	Nielsen			
		5,835,616	11/98	Lobo, et al.			
		6,212,030	07/91	Lu			
		6,461,807	12/97	Javidi			
		6,961,361	11/98	Lobo, et al.			
		7,211,138	07/91	Lu			
		7,460,916	12/97	Javidi			
		7,710,693	07/98	Nielsen			
		7,960,470	11/98	Lobo, et al.			
		8,210,247	07/91	Lu			
		8,460,024	12/97	Javidi			
		8,709,801	07/98	Nielsen			
		8,959,578	11/98	Lobo, et al.			
		9,209,355	07/91	Lu			
		9,459,132	12/97	Javidi			
		9,708,909	07/98	Nielsen			
		9,958,687	11/98	Lobo, et al.			
		~~10,208,464~~	~~07/91~~	~~Lu~~			
		~~10,458,241~~	~~12/97~~	~~Javidi~~			
		~~10,957,795~~	~~11/98~~	~~Lobo, et al.~~			
		~~11,207,572~~	~~07/91~~	~~Lu~~			
		~~11,457,349~~	~~12/97~~	~~Javidi~~			
		5,031,228	07/91	Lu			
		5,699,449	12/97	Javidi			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/22/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2003/0236832	12/03	McIntyre, et al.			
		6,678,664	01/04	Ganesan			
		6,687,390	02/04	Avni			
		6,697,502	02/04	Luo			
		6,728,401	04/04	Hardeberg			
		2004/0070678	04/04	Toyama, et al.			
		2004/0081338	04/04	Takenaka			
		2004/0125991	07/04	Yokoi			
		2004/0143598	07/04	Drucker, et al.			
		6,775,397	08/04	Hamalainen			
		2004/0190758	09/04	Doi, et al.			
		2004/0109584	10/04	Lestideau			
		2004/0201709	10/04	McIntyre, et al.			
		6,840,149	10/04	Squilla, et al.			
		20047/0264780	12/04	Zhang, et al.			
		2005/0031173	02/05	Hwang			
		2005/0065855	03/05	Geller			
		2005/0094849	05/05	Sung, et al.			
		2005/0100195	05/05	Li			
		2005/0117802	06/05	Yonaha, et al.			
		2005/0141766	06/05	Nagahashi, et al.			
		2005/0180627	08/05	Yang, et al.			
		2005/0190273	09/05	Toyama, et al.			
		2005/0220347	10/05	Enomoto			
		2005/0251015	11/05	Takikawa, et al.			
		2005/0265603	12/05	Porter, et al.			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/22/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		7,003,135	02/06	Hsieh, et al.			
		2006/0050933	03/06	Adam, et al.			
		2006/0110014	05/06	Philomin			
		2006/0133672	06/06	Li			
		2006/0156029	07/06	Algazi			
		2006/0173560	08/06	Widrow			
		2006/0218225	09/06	Hee Voon, et al.			
		2006/0222215	10/06	Jung, et al.			
		2006/0239515	10/06	Zhang, et al.			
		2006/0251292	11/06	Gokturk, et al.			
		2006/0251338	11/06	Gokturk, et al.			
		2006/0251339	11/06	Gokturk, et al.			
		2006/0253491	11/06	Gokturk, et al.			
		2006/0274978	12/06	Fukuda, et al.			
		2007/0074114	03/07	Adjali			
		2007/0081744	04/07	Gokturk, et al.			
		2007/0098303	05/07	Gallagher, et al.			
		7,218,774	05/07	Liu			
		7,231,657	06/07	Honarvar			
		~~2007/177805~~	~~08/07~~	~~Gallagher~~			
		2007/0206834	09/07	Shinkai, et al.			
		2007/0211925	09/07	Aoki, et al.			
		7,289,648	10/07	Liu			
		7,308,581	12/07	Geosimonian			
		7,333,963	02/08	Widrow, et al.			
		2008/0046458	02/08	Tseng, et al.			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/22/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2008/077595	03/08	Leebow			
		2008/0080743	04/08	Schneiderman, et al.			
		2008/0080745	04/08	Vanhoucke, et al.			
		2008/0091723	04/08	Zuckerberg, et al.			
		2008/0130960	06/08	Yagnik			
		7,415,152	08/08	Jiang, et al.			
		2008/0212849	09/08	Gao			
		2008/317379	12/08	Steinberg, et al.			
		7,519,200	04/09	Gokturk, et al.			
		2009/0185784	07/09	Hiroike, et al.			
		2009/0226052	09/09	Fedel			
		2009/232367	09/09	Shimzaki			
		2009/0252383	10/09	Adam, et al.			
		7,636,450	12/09	Bourdev			
		2009/0324018	12/09	Tell			
		2009/0324022	12/09	Sangberg, et al.			
		2009/0324137	12/09	Stallings, et al.			
		7,646,909	01/10	Jiang, et al.			
		7,660,444	02/10	Hamalainen			
		2010/0050134	02/10	Clarkson			
		20,100,067,750	03/10	Matsuo			
		2010/0054600	03/10	Anbalagan, et al.			
		2010/0054601	03/10	Anbalagan, et al.			
		2010/0061631	03/10	Omori			
		2010/0158327	06/10	Kangas, et al.			
		7,788,247	08/10	Wang, et al.			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/22/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2010/0232656	09/10	Ryu			
		7,804,982	09/10	Howard, et al.			
		~~2010/245614~~	~~09/10~~	~~Matsunaga~~			
		7,809,722	10/10	Gokturk, et al.			
		~~2010/272363~~	~~10/10~~	~~Steinberg, et al.~~			
		2010/0287053	11/10	Ganong, et al.			
		2010/0318366	12/10	Sullivan			
		2010/0317420	12/10	Hoffberg			
		~~2,011,063,108~~	~~03/11~~	~~Aonuma, et al.~~			
		7,945,653	05/11	Zuckerberg, et al.			
		2011/0169853	07/11	Oiwa			
		2011/0202531	08/11	Zuckerberg, et al.			
		2011/0225481	09/11	Zuckerberg, et al.			
		2011/0282906	11/11	Wong			
		~~D650,793~~	~~12/11~~	~~Impas~~			
		8,121,408	02/12	Omori			
		8,165,352	04/12	Mohanty, et al.			
		8,244,211	08/12	Clark			
		~~D667,423~~	~~09/12~~	~~Nagamine~~			
		8,316,237	11/12	Felsher, et al.			
		2012/0323704	12/12	Steelberg			
		8,326,000	12/12	Jung, et al.			
		2013/0007032	01/13	Klappert			
		2013/0066526	03/13	Mondragon			
		8,392,268	03/13	Smith, et al.			
		~~2013/057693~~	~~03/13~~	~~Baranek~~			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/22/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		8,396,246	03/13	Anbalagan, et al.			
		~~2013/077835~~	~~03/13~~	~~Krim, et al.~~			
		8,416,312	04/13	Matsunaga			
		2013/0179298	07/13	Segman			
		2013/0226740	08/13	Biliosa			
		2013/0246158	09/13	Cannon			
		2013/0267204	10/13	Schultz			
		2013/0342672	12/13	Gray, et al.			
		2014/0012756	01/14	Beraja			
		2014/0059673	02/14	Azar			
		8,649,604	02/14	Steinberg, et al.			
		~~214/0098174~~	~~04/14~~	~~Summers~~			
		2014/0118257	05/14	Baldwin			
		2014/0165187	06/14	Daesung			
		2014/0169643	06/14	Todoroki			
		8,743,051	06/14	Moy, et al.			
		8,750,574	06/14	Ganong, et al.			
		2014/0198959	07/14	Derakhshani			
		8,788,977	07/14	Bezos			
		8,856,541	10/14	Chaudhury			
		8,867,849	10/14	Kirkham			
		2014/0337948	11/14	Hoyos			
		8,922,480	12/14	Freed, et al.			
		2015/0052462	02/15	Kulkarni			
		2015/0055821	02/15	Fotland			
		2015/0077323	03/15	Ramaswamy			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/22/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		~~D726,221~~	~~04/15~~	~~Gomez~~			
		9,037,354	05/15	Mondragon			
		2015/0131872	05/15	Ganong, et al.			
		2015/0153571	06/15	Ballard			
		9,076,028	07/15	Summers			
		9,076,008	07/15	Moy			
		~~D737,325~~	~~08/15~~	~~Kim~~			
		9,137,246	09/15	Parry, et al.			
		2015/0310260	10/15	Summers			
		9,152,849	10/15	Ganong, et al.			
		9,202,105	12/15	Wang, et al.			
		2015/0378433	12/15	Savastinuk			
		2016/0063235	03/16	Tussy			
		~~D753,132~~	~~04/16~~	~~Cuthbert~~			
		~~D756,401~~	~~05/16~~	~~Soldner~~			
		2016/0209939	07/16	Zambetti			
		9,424,491	08/16	Kirkham			
		9,430,695	08/16	Summers			
		~~D762,655~~	~~08/16~~	~~Kai~~			
		~~D762,673~~	~~08/16~~	~~Seo~~			
		~~D762,715~~	~~08/16~~	~~Williamson~~			
		~~D763,271~~	~~08/16~~	~~Everette~~			
		2016/0259528	09/16	Foss			
		2016/0261675	09/16	Block			
		~~D765,674~~	~~09/16~~	~~Kim~~			
		~~D769,933~~	~~10/16~~	~~Sabia~~			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/22/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2016/0342826	11/16	Apostolos, et al.			
		~~D776,680~~	~~01/17~~	~~Bae~~			
		~~D778,923~~	~~02/17~~	~~Zhou~~			
		D778,940	02/17	Williamson			
		9,607,138	03/17	Baldwin			
		~~D780,781~~	~~03/17~~	~~Ding~~			
		9,600,649	03/17	Parry, et al.			
		~~D783,633~~	~~04/17~~	~~Oh~~			
		~~D783,652~~	~~04/17~~	~~Guan~~			
		~~D784,363~~	~~04/17~~	~~Fleming~~			
		~~D787,527~~	~~05/17~~	~~Wilberding~~			
		D788,122	05/17	Tada			
		9,740,848	08/17	Parry, et al.			
		2017/0220843	08/17	Apostolos, et al.			

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
							YES	NO
		EP 1388802	02/04	Europe			X	
		EP 1455297	09/04	Europe			X	
		WO 2006/130542	12/06	WIPO			X	
		WO 2008/107002	09/08	WIPO			X	
		WO 2015/070320	05/15	WIPO			X	

EXAMINER INITIAL	**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)
	After Effects Tutorial - 17 - Introduction to Masking, by thenewboston, uploaded 12/07/2008, youtube.com [online], [retrieved 06/15/2017]. Available from <URL:https://www.youtube.com/watch?v=kWd51xDqzIc>

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/22/2017

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

EXAMINER INITIAL		**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)
		Optical Illusions - Animated GIF & JPG, dated 10/28/2013, plus.google.com [online], [retrieved 06/19/2017]. Available from internet <URL:https://plus.google.com/+Whak-Off/posts/CX4YhzXSQy2>
		The Universal Face Login for 5 Billion Smartphones, zoomlogin.com [online], [retrieved 06/19/2017]. Available from internet <URL:https://zoomlogin.com/>
		Wong, Yongkang, et al. "Patch-based probabilistic image quality assessment for face selection and improved video-based face recognition." CVPR 2011 WORKSHOPS. IEEE, 2011
		RAFALOVITCH, "Viewfinder Friends-idea for Facebook application", November 14, 2007, http://blog.outerthoughts.com/2007/11/viewfinder-friends-idea-for-facebook-application/, 5pages.
		KISHORE, "How to Add, Upload, and Tag Your Pictures and Photos in FaceBook", http://www.online-tech-tips.com/fun-stuff/how-to-add-upload-and-tag-your-pictures-and-photos-in-facebook/, August 11, 2007, 13 pages.
		BECKER et al., "Evaluation of Face Recognition Techniques for Application to Facebook", IEEE International conference on Automatic Face and Gesture Recognition, 2008, 6 pages.
		BAKER, "Google & Riya Face Recognition Photo Search", November 22, 2005, http://www.searchenginejournal.com/google-riya-face-recognition-photo-search/25501, 1 page_
		PONCE, "Riya, Photo Sharing with Face Recognition", October 28, 2005, http://www.ohgizmo.com/2005/10/28/riya-photo-sharing-with-face-recognition/, 2 pages_
		FACEBOOK, "Making Photo Tagging Easier", https://m.facebook.com/notes/facebook/making-photo-tagging-easier/467145887130/?_tn_=C&_rdr, 2 pages
		MICHELSON et al., "Auto-tagging the Facebook", 2006, http://cs229.stanford.edu/proj2006/MichelsonOrtiz-AutoTaggingTheFacebook.pdf, 5 pages.
		ARRINGTON, "First Screen Shots of Riya", October 26, 2005, http://techcrunch.com/2005/10/26/riya-prepares-to-launch-alpha/, 10 pages
		ARRINGTON, "Ojos - Auto Name & Tag Your Photos", August 15, 2005, http://techcrunch.com/2005/08/31/ojos-auto-name-tag-your-photos/, 8 pages.
		STONE, et al. "Autotagging Facebook: Social network context improves photo annotation," In Workshop on Internet Vision, 2008, 2 pages_
		SCHUON et al., "CS229 Project Report: Automated photo tagging in Facebook", December 2007, http://cs229.Stanford.edu/proj2007/SchuonRobertsonZou-AutomatedPhotoTaggingInFacebook.pdf, 5 pages.
		YADAV, "Facebook - The Complete Biography", August 25, 2006, http://mashable.com12006/08/25/facebook-protile/, 7 pages_
		UNKNOWN, "What does it mean to "tag" someones picture on facebook, whats the point of doing it?", November 28, 2007, https://answers.yahoo.com/question/index?qid=20071128123629AAY0DLP, 2 pages.
		Yang, et al., "Detecting Faces in Images: A Survey", January 2002, IEEE Trans. Pattern Analysis Machine Intelligence, 24(1), 2 pages

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/22/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address : COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
14/839,505	28 August, 2015	TUSSY, KEVIN ALAN	FACIAL.0012P

WEIDE & MILLER, LTD.
10655 Park Run Drive
SUITE 100
LAS VEGAS, NV 89144

EXAMINER	
SHANTO M. ABEDIN	
ART UNIT	PAPER
2436	20171223

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

The information disclosure statement (IDS) submitted on 09/29/2017 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner. Please note some IDS documents can not be retreived by the examiner and are not considerd (crossed out) as they seem to contain incorrect document number.
See Attached and newly annotated IDS (09/29/2017).

/SHANTO M ABEDIN/
Primary Examiner, Art Unit 2436

PTO-90C (Rev.04-03)

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		5,031,228	07/91	Lu			
		5,699,449	12/97	Javidi			
		5,784,056	07/98	Nielsen			
		5,835,616	11/98	Lobo, et al.			
		6,212,030	07/91	Lu			
		6,461,807	12/97	Javidi			
		6,961,361	11/98	Lobo, et al.			
		7,211,138	07/91	Lu			
		7,460,916	12/97	Javidi			
		7,710,693	07/98	Nielsen			
		7,960,470	11/98	Lobo, et al.			
		8,210,247	07/91	Lu			
		8,460,024	12/97	Javidi			
		8,709,801	07/98	Nielsen			
		8,959,578	11/98	Lobo, et al.			
		9,209,355	07/91	Lu			
		9,459,132	12/97	Javidi			
		9,708,909	07/98	Nielsen			
		9,958,687	11/98	Lobo, et al.			
		~~10,208,464~~	~~07/91~~	~~Lu~~			
		~~10,458,241~~	~~12/97~~	~~Javidi~~			
		~~10,957,795~~	~~11/98~~	~~Lobo, et al.~~			
		~~11,207,572~~	~~07/91~~	~~Lu~~			
		~~11,457,349~~	~~12/97~~	~~Javidi~~			
		5,031,228	07/91	Lu			
		5,699,449	12/97	Javidi			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/22/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2003/0236832	12/03	McIntyre, et al.			
		6,678,664	01/04	Ganesan			
		6,687,390	02/04	Avni			
		6,697,502	02/04	Luo			
		6,728,401	04/04	Hardeberg			
		2004/0070678	04/04	Toyama, et al.			
		2004/0081338	04/04	Takenaka			
		2004/0125991	07/04	Yokoi			
		2004/0143598	07/04	Drucker, et al.			
		6,775,397	08/04	Hamalainen			
		2004/0190758	09/04	Doi, et al.			
		2004/0109584	10/04	Lestideau			
		2004/0201709	10/04	McIntyre, et al.			
		6,840,149	10/04	Squilla, et al.			
		~~20047/0264780~~	~~12/04~~	~~Zhang, et al.~~			
		2005/0031173	02/05	Hwang			
		2005/0065855	03/05	Geller			
		2005/0094849	05/05	Sung, et al.			
		2005/0100195	05/05	Li			
		2005/0117802	06/05	Yonaha, et al.			
		2005/0141766	06/05	Nagahashi, et al.			
		2005/0180627	08/05	Yang, et al.			
		2005/0190273	09/05	Toyama, et al.			
		2005/0220347	10/05	Enomoto			
		2005/0251015	11/05	Takikawa, et al.			
		2005/0265603	12/05	Porter, et al.			

EXAMINER	/SHANTO ABEDIN/	DATE CONSIDERED	12/22/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		7,003,135	02/06	Hsieh, et al.			
		2006/0050933	03/06	Adam, et al.			
		2006/0110014	05/06	Philomin			
		2006/0133672	06/06	Li			
		2006/0156029	07/06	Algazi			
		2006/0173560	08/06	Widrow			
		2006/0218225	09/06	Hee Voon, et al.			
		2006/0222215	10/06	Jung, et al.			
		2006/0239515	10/06	Zhang, et al.			
		2006/0251292	11/06	Gokturk, et al.			
		2006/0251338	11/06	Gokturk, et al.			
		2006/0251339	11/06	Gokturk, et al.			
		2006/0253491	11/06	Gokturk, et al.			
		2006/0274978	12/06	Fukuda, et al.			
		2007/0074114	03/07	Adjali			
		2007/0081744	04/07	Gokturk, et al.			
		2007/0098303	05/07	Gallagher, et al.			
		7,218,774	05/07	Liu			
		7,231,657	06/07	Honarvar			
		2007/177805	08/07	Gallagher			
		2007/0206834	09/07	Shinkai, et al.			
		2007/0211925	09/07	Aoki, et al.			
		7,289,648	10/07	Liu			
		7,308,581	12/07	Geosimonian			
		7,333,963	02/08	Widrow, et al.			
		2008/0046458	02/08	Tseng, et al.			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/22/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		~~2008/077393~~	~~03/08~~	~~Leebow~~			
		2008/0080743	04/08	Schneiderman, et al.			
		2008/0080745	04/08	Vanhoucke, et al.			
		2008/0091723	04/08	Zuckerberg, et al.			
		2008/0130960	06/08	Yagnik			
		7,415,152	08/08	Jiang, et al.			
		2008/0212849	09/08	Gao			
		~~2008/317379~~	~~12/08~~	~~Steinberg, et al.~~			
		7,519,200	04/09	Gokturk, et al.			
		2009/0185784	07/09	Hiroike, et al.			
		2009/0226052	09/09	Fedel			
		~~2009/232367~~	~~09/09~~	~~Shinzaki~~			
		2009/0252383	10/09	Adam, et al.			
		7,636,450	12/09	Bourdev			
		2009/0324018	12/09	Tell			
		2009/0324022	12/09	Sangberg, et al.			
		2009/0324137	12/09	Stallings, et al.			
		7,646,909	01/10	Jiang, et al.			
		7,660,444	02/10	Hamalainen			
		2010/0050134	02/10	Clarkson			
		~~20,100,067,750~~	~~03/10~~	~~Matsuo~~			
		2010/0054600	03/10	Anbalagan, et al.			
		2010/0054601	03/10	Anbalagan, et al.			
		2010/0061631	03/10	Omori			
		2010/0158327	06/10	Kangas, et al.			
		7,788,247	08/10	Wang, et al.			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/22/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2010/0232656	09/10	Ryu			
		7,804,982	09/10	Howard, et al.			
		~~2010/245614~~	~~09/10~~	~~Matsunaga~~			
		7,809,722	10/10	Gokturk, et al.			
		~~2010/272363~~	~~10/10~~	~~Steinberg, et al.~~			
		2010/0287053	11/10	Ganong, et al.			
		2010/0318366	12/10	Sullivan			
		2010/0317420	12/10	Hoffberg			
		~~2,011,063,108~~	~~03/11~~	~~Aonuma, et al.~~			
		7,945,653	05/11	Zuckerberg, et al.			
		2011/0169853	07/11	Oiwa			
		2011/0202531	08/11	Zuckerberg, et al.			
		2011/0225481	09/11	Zuckerberg, et al.			
		2011/0282906	11/11	Wong			
		D650,793	12/11	Impas			
		8,121,408	02/12	Omori			
		8,165,352	04/12	Mohanty, et al.			
		8,244,211	08/12	Clark			
		D667,423	09/12	Nagamine			
		8,316,237	11/12	Felsher, et al.			
		2012/0323704	12/12	Steelberg			
		8,326,000	12/12	Jung, et al.			
		2013/0007032	01/13	Klappert			
		2013/0066526	03/13	Mondragon			
		8,392,268	03/13	Smith, et al.			
		~~2013/057693~~	~~03/13~~	~~Baranek~~			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/22/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		8,396,246	03/13	Anbalagan, et al.			
		~~2013/077835~~	~~03/13~~	~~Krim, et al.~~			
		8,416,312	04/13	Matsunaga			
		2013/0179298	07/13	Segman			
		2013/0226740	08/13	Biliosa			
		2013/0246158	09/13	Cannon			
		2013/0267204	10/13	Schultz			
		2013/0342672	12/13	Gray, et al.			
		2014/0012756	01/14	Beraja			
		2014/0059673	02/14	Azar			
		8,649,604	02/14	Steinberg, et al.			
		~~214/0098174~~	~~04/14~~	~~Summers~~			
		2014/0118257	05/14	Baldwin			
		2014/0165187	06/14	Daesung			
		2014/0169643	06/14	Todoroki			
		8,743,051	06/14	Moy, et al.			
		8,750,574	06/14	Ganong, et al.			
		2014/0198959	07/14	Derakhshani			
		8,788,977	07/14	Bezos			
		8,856,541	10/14	Chaudhury			
		8,867,849	10/14	Kirkham			
		2014/0337948	11/14	Hoyos			
		8,922,480	12/14	Freed, et al.			
		2015/0052462	02/15	Kulkarni			
		2015/0055821	02/15	Fotland			
		2015/0077323	03/15	Ramaswamy			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/22/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		D726,221	04/15	Gomez			
		9,037,354	05/15	Mondragon			
		2015/0131872	05/15	Ganong, et al.			
		2015/0153571	06/15	Ballard			
		9,076,028	07/15	Summers			
		9,076,008	07/15	Moy			
		D737,325	08/15	Kim			
		9,137,246	09/15	Parry, et al.			
		2015/0310260	10/15	Summers			
		9,152,849	10/15	Ganong, et al.			
		9,202,105	12/15	Wang, et al.			
		2015/0378433	12/15	Savastinuk			
		2016/0063235	03/16	Tussy			
		D753,132	04/16	Cuthbert			
		D756,401	05/16	Soldner			
		2016/0209939	07/16	Zambetti			
		9,424,491	08/16	Kirkham			
		9,430,695	08/16	Summers			
		D762,655	08/16	Kai			
		D762,673	08/16	Seo			
		D762,715	08/16	Williamson			
		D763,271	08/16	Everette			
		2016/0259528	09/16	Foss			
		2016/0261675	09/16	Block			
		D765,674	09/16	Kim			
		D769,933	10/16	Sabia			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/22/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2016/0342826	11/16	Apostolos, et al.			
		D776,680	01/17	Bae			
		D778,923	02/17	Zhou			
		D778,940	02/17	Williamson			
		9,607,138	03/17	Baldwin			
		D780,781	03/17	Ding			
		9,600,649	03/17	Parry, et al.			
		D783,633	04/17	Oh			
		D783,652	04/17	Guan			
		D784,363	04/17	Fleming			
		D787,527	05/17	Wilberding			
		D788,122	05/17	Tada			
		9,740,848	08/17	Parry, et al.			
		2017/0220843	08/17	Apostolos, et al.			

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
							YES	NO
		EP 1388802	02/04	Europe			X	
		EP 1455297	09/04	Europe			X	
		WO 2006/130542	12/06	WIPO			X	
		WO 2008/107002	09/08	WIPO			X	
		WO 2015/070320	05/15	WIPO			X	

EXAMINER INITIAL	**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)
	After Effects Tutorial - 17 - Introduction to Masking, by thenewboston, uploaded 12/07/2008, youtube.com [online], [retrieved 06/15/2017]. Available from <URL:https://www.youtube.com/watch?v=kWd51xDqzIc>

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/22/2017

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

EXAMINER INITIAL		**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)
		Optical Illusions - Animated GIF & JPG, dated 10/28/2013, plus.google.com [online], [retrieved 06/19/2017]. Available from internet <URL:https://plus.google.com/+Whak-Off/posts/CX4YhzXSQy2>
		The Universal Face Login for 5 Billion Smartphones, zoomlogin.com [online], [retrieved 06/19/2017]. Available from internet <URL:https://zoomlogin.com/>
		Wong, Yongkang, et al. "Patch-based probabilistic image quality assessment for face selection and improved video-based face recognition." CVPR 2011 WORKSHOPS. IEEE, 2011
		RAFALOVITCH, "Viewfinder Friends-idea for Facebook application", November 14, 2007, http://blog.outerthoughts.com/2007/11/viewfinder-friends-idea-for-facebook-application/, 5pages.
		KISHORE, "How to Add, Upload, and Tag Your Pictures and Photos in FaceBook", http://www.online-tech-tips.com/fun-stuff/how-to-add-upload-and-tag-your-pictures-and-photos-in-facebook/, August 11, 2007, 13 pages.
		BECKER et al., "Evaluation of Face Recognition Techniques for Application to Facebook", IEEE International conference on Automatic Face and Gesture Recognition, 2008, 6 pages.
		BAKER, "Google & Riya Face Recognition Photo Search", November 22, 2005, http://www.searchenginejournal.com/google-riya-face-recognition-photo-search/25501, 1 page_
		PONCE, "Riya, Photo Sharing with Face Recognition", October 28, 2005, http://www.ohgizmo.com/2005/10/28/riya-photo-sharing-with-face-recognition/, 2 pages_
		FACEBOOK, "Making Photo Tagging Easier", https://m.facebook.com/notes/facebook/making-photo-tagging-easier/467145887130/?_tn_=C&_rdr, 2 pages
		MICHELSON et al., "Auto-tagging the Facebook", 2006, http://cs229.stanford.edu/proj2006/MichelsonOrtiz-AutoTaggingTheFacebook.pdf, 5 pages.
		ARRINGTON, "First Screen Shots of Riya", October 26, 2005, http://techcrunch.com/2005/10/26/riya-prepares-to-launch-alpha/, 10 pages
		ARRINGTON, "Ojos - Auto Name & Tag Your Photos", August 15, 2005, http://techcrunch.com/2005/08/31/ojos-auto-name-tag-your-photos/, 8 pages.
		STONE, et al. "Autotagging Facebook: Social network context improves photo annotation," In Workshop on Internet Vision, 2008, 2 pages_
		SCHUON et al., "CS229 Project Report: Automated photo tagging in Facebook", December 2007, http://cs229.Stanford.edu/proj2007/SchuonRobertsonZou-AutomatedPhotoTaggingInFacebook.pdf, 5 pages.
		YADAV, "Facebook - The Complete Biography", August 25, 2006, http://mashable.com12006/08/25/facebook-protile/, 7 pages_
		UNKNOWN, "What does it mean to "tag" someones picture on facebook, whats the point of doing it?", November 28, 2007, https://answers.yahoo.com/question/index?qid=20071128123629AAY0DLP, 2 pages.
		Yang, et al., "Detecting Faces in Images: A Survey", January 2002, IEEE Trans. Pattern Analysis Machine Intelligence, 24(1), 2 pages

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/22/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

32856 7590 12/15/2017

WEIDE & MILLER, LTD.
10655 Park Run Drive
SUITE 100
LAS VEGAS, NV 89144

EXAMINER
ABEDIN, SHANTO

ART UNIT	PAPER NUMBER
2436	

DATE MAILED: 12/15/2017

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/839,505	08/28/2015	Kevin Alan Tussy	FACIAL.0012P	6236

TITLE OF INVENTION: Facial Recognition Authentication System Including Path Parameters

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	03/15/2018

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

32856 7590 12/15/2017
WEIDE & MILLER, LTD.
10655 Park Run Drive
SUITE 100
LAS VEGAS, NV 89144

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/839,505	08/28/2015	Kevin Alan Tussy	FACIAL.0012P	6236

TITLE OF INVENTION: Facial Recognition Authentication System Including Path Parameters

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	03/15/2018

EXAMINER	ART UNIT	CLASS-SUBCLASS
ABEDIN, SHANTO	2436	726-006000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): (**Please first reapply any previously paid issue fee shown above**)
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29
  NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27
  NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status.
  NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/839,505	08/28/2015	Kevin Alan Tussy	FACIAL.0012P	6236

32856 7590 12/15/2017

WEIDE & MILLER, LTD.
10655 Park Run Drive
SUITE 100
LAS VEGAS, NV 89144

EXAMINER	
ABEDIN, SHANTO	
ART UNIT	**PAPER NUMBER**
2436	

DATE MAILED: 12/15/2017

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	14/839,505	TUSSY, KEVIN ALAN	
	Examiner	Art Unit	
	SHANTO M. ABEDIN	2436	

All participants (applicant, applicant's representative, PTO personnel):

(1) *SHANTO M. ABEDIN*. (3)_____.

(2) *CHAD W. MILLER (Reg No. 44,943)*. (4)_____.

Date of Interview: *06 December 2017*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☐103 ☒Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1,7 and 22*.

Identification of prior art discussed: *NONE*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant's representative was contacted regarding proposed examiner's amendments to the independent claims in order to place the application in condition for allowance. An agreement was reached regarding the proposed examiner's amendments .

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/SHANTO M ABEDIN/ Primary Examiner, Art Unit 2436	

Notice of Allowability	Application No. 14/839,505	Applicant(s) TUSSY, KEVIN ALAN	
	Examiner SHANTO M. ABEDIN	Art Unit 2436	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *filing of 10/05/2017*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-14 and 22-27*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 09/29/2017
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date *12/06/2017* .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/SHANTO M ABEDIN/
Primary Examiner, Art Unit 2436

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

DETAILED ACTION

1. This is in response to the communication filed on 10/05/2017. Claims 1-14 and 22-27 were pending in the application. Claims 1-14 and 22-27 have been allowed.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 09/29/2017 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Examiner's Amendment

3. An examiner's amendment to the record appears below. Should the changes and/ or additions be unacceptable to the applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee. Authorization for this examiner's amendment was given in a telephone interview with the applicant's representative Mr. Chad W. Miller (Reg. No. 44,943) on 12/06/2017. Claims 1, 7-8, 22 and 26 have been amended as follows:

Claim 1. **(Currently amended)** A method for enrolling and authenticating a user in an authentication system via the user's a mobile device comprising a camera and at least one movement detecting sensor, the mobile device also having a display, the method comprising:

capturing enrollment biometric information from at least one first image of the user, the first image recorded by the camera of the mobile device;

storing the enrollment biometric information on a memory;

during an authentication session:

capturing authentication biometric information from at least one second image of the user, the second image recorded by the camera of the mobile device;

recording path parameter data from the at least one movement detecting sensor in the mobile device, the path parameter data generated by movement of the mobile device by the user and representing an authentication movement of the mobile device;

comparing the authentication biometric information to the stored enrollment biometric information to determine whether the authentication biometric information meets a predetermine similarity threshold as compared to the enrollment biometric information;

comparing the authentication movement of the mobile device to an expected movement of the mobile device to determine whether the authentication movement meets a predetermine similarity threshold as compared to the expected movement of the mobile device by the user, wherein the expected movement is based on a path of the mobile device that includes having a face of the user appear in a display area of the mobile device; and

when the authentication biometric information sufficiently corresponds with the enrollment biometric information, and when the authentication movement meets a predetermine similarity threshold as compared to the expected movement, authenticating the user.

Claim 7. **(Currently amended)** A facial authentication system utilizing a user's mobile device, the mobile device comprising a camera and at least one movement detecting sensor, the authentication system comprising:

an authentication server comprising a processor, a memory, and at least one transceiver configured to transmit data from the authentication server and received data;

one or more memories configured to store one or more databases, the one or more databases configured to store authentication information profiles; and

machine readable instructions that are stored on the memory of the authentication server which when executed by the processor, cause the authentication server to:

receive enrollment biometrics from the mobile device, the enrollment biometrics comprising facial recognition data processed from at least one first image of the user's face obtained via the camera of the mobile device;

store the enrollment biometrics in the one or more databases and associate the enrollment biometrics ~~data~~ with the user authentication information profile;

receive authentication biometrics from the mobile device during an authentication attempt by the user, the authentication biometrics comprising facial recognition data processed from at least one second image of the user's face, the image obtained from the camera of the mobile device;

receive authentication movement information from the mobile device, the authentication movement information comprising data regarding movement of the mobile device by the user as detected by the at least one movement detecting sensor in the mobile device;

compare the authentication biometrics and the authentication movement information with the enrollment biometrics and expected movement information stored in the database with the user

authentication information profile, wherein ~~such that~~ the expected movement is based on an anticipated path of the mobile device, due to movement of the mobile device by the user, to place the user's face sequentially in a first display area and a second display area; and

authenticate or not authenticate the user based on a comparison match rate of the authentication biometrics and the authentication movement with the enrollment biometrics and the expected movement.

Claim 8. **(Currently amended)** The facial authentication system of claim 7, wherein the mobile device displays a first prompt on a display screen to instruct the user to position the user's face within the first display area of the display screen; and ~~,~~

the mobile device displays a second prompt on the display screen to instruct the user to position the user's face within the second display area of the display screen, the second display area being a different size than the first display area.

Claim 10. **(Currently amended)** The facial authentication system of claim 7, wherein the authentication server detects ~~detect~~ the present or absence of a screen edge in the at least one second image.

Claim 22. **(Currently amended)** A facial authentication system utilizing a user's mobile device, the mobile device comprising a camera and at least one movement detecting sensor, the authentication system comprising:

a processor located in the mobile device configured to execute machine readable instructions;

one or more memories in the mobile device storing authentication information; and

non-transitory machine readable instructions, the machine readable instructions when executed by the processor cause the mobile device to:

receive enrollment biometrics, the enrollment biometrics comprising facial recognition data processed from at least one first image of the user's face obtained via the camera of the mobile device;

store the enrollment biometrics in the memory of the mobile device and associate the enrollment biometrics ~~data~~ with a ~~the~~ user profile of the user;

receive authentication biometrics from the mobile device during an authentication attempt by the user, the authentication biometrics comprising facial recognition data processed from at least one second image of the user's face, the image obtained from the camera of the mobile device during the authentication attempt;

receive authentication movement information from the mobile device, the authentication movement information comprising data generated during movement of the mobile device by the user during the authentication attempt as detected by the at least one movement detecting sensor in the mobile device;

compare the authentication biometrics and the authentication movement information with the enrollment biometrics and expected movement information stored in the mobile device, wherein ~~such that~~ the expected movement information is based on an anticipated path of the mobile device to place the user's face sequentially in a first display area and a second display area; and

authenticate or not authenticate the user during the authentication attempt based on a comparison match rate of the authentication biometrics and the authentication movement information with the enrollment biometrics and the expected movement information.

Claim 26. (Currently amended) The system of claim 22 wherein the anticipated path of the mobile device is a path of the mobile device between a first mobile device position and a

second mobile device position, wherein ~~such that~~ the first position is a different distance from the user than the second distance.

Examiner's Reasons for Allowance

4. The following is an examiner's statement of reasons for allowances:

Independent claim 1 is patentable over the cited prior arts because they do not anticipate nor fairly and reasonably teach independently or in combination a method comprising besides other limitations: capturing authentication biometric information from at least one second image of the user; and recording path parameter data from one movement detecting sensor in the mobile device, the path parameter data generated by movement of the mobile device by the user and representing an authentication movement of the mobile device; and comparing the authentication movement of the mobile device to an expected movement of the mobile device to determine whether the authentication movement meets a predetermine similarity threshold as compared to the expected movement of the mobile device, wherein the expected movement is based on a path of the mobile device that includes having a face of the user appear in a display area of the mobile device; and when the authentication biometric information sufficiently corresponds with the enrollment biometric information, and when the authentication movement meets a predetermine similarity threshold as compared to the expected movement, authenticating the user.

Independent claim 7 is patentable over the cited prior arts because they do not anticipate nor fairly and reasonably teach independently or in combination a system comprising besides other limitations: cause the authentication server to: receive authentication biometrics comprising facial recognition data processed from at least one second image of the user's face; and receive

authentication movement information from the mobile device, the authentication movement information comprising data regarding movement of the mobile device by the user as detected by the at least one movement detecting sensor in the mobile device; and compare the authentication biometrics and the authentication movement information with the enrollment biometrics and expected movement information stored in the database with the user authentication information profile, wherein the expected movement is based on an anticipated path of the mobile device, due to movement of the mobile device by the user, to place the user's face sequentially in a first display area and a second display area; and authenticate or not authenticate the user based on a comparison match rate of the authentication biometrics and the authentication movement with the enrollment biometrics and the expected movement.

Independent claim 22 is patentable over the cited prior arts because they do not anticipate nor fairly and reasonably teach independently or in combination a system comprising besides other limitations: cause the mobile device to: receive authentication biometrics comprising facial recognition data processed from at least one second image of the user's face; and receive authentication movement information comprising data generated during movement of the mobile device by the user as detected by the at least one movement detecting sensor in the mobile device; and compare the authentication biometrics and the authentication movement information with the enrollment biometrics and expected movement information stored in the mobile device, wherein the expected movement information is based on an anticipated path of the mobile device to place the user's face sequentially in a first display area and a second display area; and authenticate or not authenticate the user during the authentication attempt based on a comparison match rate of the

authentication biometrics and the authentication movement information with the enrollment biometrics and the expected movement information.

Response to Arguments

5. Applicant's arguments, see remarks, filed on 10/05/2017, with respect to 35 USC 103 type rejections of claims 1-6 have been fully considered and are persuasive. Previous 35 USC 103 type rejections of claims 1-6 have been withdrawn. Applicant's arguments, see remarks, filed on 10/05/2017, with respect to 35 USC 103 type rejections of claims 7-14 have been fully considered and are persuasive. Previous 35 USC 103 type rejections of claims 7-14 have been withdrawn. Applicant's arguments, see remarks, filed on 10/05/2017, with respect to 35 USC 103 type rejections of claims 15-21 have been fully considered and are persuasive. Previous 35 USC 103 type rejections of claims 15-21 are now moot because of cancellation of these claims.

Conclusion

6. Claims 1-14 and 22-27 are patentable.

7. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M. Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 10:00 AM to 6:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Shewaye Gelagay, can be reached on 571-

272-4219. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/SHANTO M ABEDIN/

Primary Examiner, Art Unit 2436

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	14/839,505	TUSSY, KEVIN ALAN	
	Examiner	Art Unit	
	SHANTO M. ABEDIN	2436	

All participants (applicant, applicant's representative, PTO personnel):

(1) *SHANTO M. ABEDIN*. (3)_____.

(2) *CHAD W. MILLER (Reg No. 44,943)*. (4)_____.

Date of Interview: *06 December 2017*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☐103 ☒Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1,7 and 22*.

Identification of prior art discussed: *NONE*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant's representative was contacted regarding proposed examiner's amendments to the independent claims in order to place the application in condition for allowance. An agreement was reached regarding the proposed examiner's amendments .

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/SHANTO M ABEDIN/ Primary Examiner, Art Unit 2436	

Notice of References Cited	Application/Control No. 14/839,505	Applicant(s)/Patent Under Reexamination TUSSY, KEVIN ALAN	
	Examiner SHANTO M. ABEDIN	Art Unit 2436	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2013/0342672 A1	12-2013	Gray; Timothy T.	G06F3/013	348/78
*	B	US-2014/0197922 A1	07-2014	Stanwood; Kenneth	G06F21/32	340/5.83
	C	US-				
	D	US-				
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Live **face detection** based on the analysis of fourier spectra

J Li, Y Wang, T Tan, AK Jain - Proc. of SPIE Vol, 2004 - proceedings.spiedigitallibrary.org

... Using structure and **movement** information of live **face**, an effective live **face detection** algorithm is presented ... a fake **face** before the **camera**, we move it according to some styles: **moving** quickly, **moving** slowly or ... The subjects sit down before the **camera** and move as they wish ...

☆ 99 Cited by 256 Related articles All 11 versions

Modelling **facial** colour and identity with gaussian mixtures

SJ McKenna, S Gong, Y Raja - Pattern **recognition**, 1998 - Elsevier

... on mR\ in the image domain at time t. The dimensions of this search **area** are determined ... Figure 2 shows a sequence of a **face** being tracked with a **moving camera** against a cluttered background ... The **camera** can be driven by maintain- ing the mean **position**, m, at the centre of ...

☆ 99 Cited by 313 Related articles All 13 versions

Unobtrusive multimodal **biometric authentication**: The HUMABIO project concept

IG Damousis, D Tzovaras, E Bekiaris - EURASIP journal on advances in ..., 2008 - Springer

... ments, walking, head **movement**, and so forth ... 7 a temporal median filter on the image sequence, assuming static background and **moving** foreground ... 5(a). In the proposed framework, 2.5D information is available since the gait sequence is captured by a stereoscopic **camera** ...

☆ 99 Cited by 48 Related articles All 10 versions »

Local binary patterns as an image preprocessing for **face authentication**

G Heusch, Y Rodriguez, S Marcel - ... and Gesture **Recognition** ..., 2006 - ieeexplore.ieee.org

... Since over 30 years, **face recognition** has been an active research **area** and different systems ... ground, controlled lighting), degraded (webcam, non- uniform background) and adverse (high-quality **camera**, arbitrary conditions ... A texture- based method for detecting **moving** objects ...

☆ 99 Cited by 211 Related articles All 21 versions »

Digital **camera** with **biometric** security

E Steinberg, Y Prilutsky - US Patent 6,433,818, 2002 - Google Patents

... use, or if the allowance is simply for a total amount of operation time, the **display** 47 would ... If **movement** is detected 202, the pattern is tested for a match with signature data 112 ... 2002, Oct 7, 2008, Mason Ricardo Storm, Portable device having a torch and a **camera** located between ...

☆ 99 Cited by 173 Related articles All 2 versions

Non-intrusive iris image capturing system using light stripe projection and pan-tilt-zoom **camera**

S Yoon, HG Jung, JK Suhr, J Kim - ... and Pattern **Recognition** ..., 2007 - ieeexplore.ieee.org

... A fisheye lens is used here to observe wide operating **area** ... And depth of field is 5–9.5cm so that this system is robust to small **movement** of user. Fig ... After tilting for **face detection**, the distance D between pan-tilt-zoom **camera** and user's **face** can be calculated ...

☆ 99 Cited by 40 Related articles All 9 versions

Applying **biometric** principles to avatar **recognition**

ML Gavrilova, R Yampolskiy - Transactions on computational science XII, 2011 - Springer

... take a look at techniques for collecting and classifying data- bases of avatars and bots, **moving** on to ... and requests the user to center the avatar's **face** with the horizon using the **movement** control ... and leg height all must be set to 50% in order to preserve the **camera** angle, which ...

☆ 99 Cited by 46 Related articles All 17 versions »

Liveness **detection** for **face recognition**

G Pan, Z Wu, L Sun - Recent advances in **face recognition**, 2008 - intechopen.com

… However, spoofing attack (or copy attack) is still a fatal threat for **biometric authentication** systems (Schukers, 2002) … Head **movement** High No Middle … photo of front view is taken for each person, then five categories of the photo-attacks are simulated before the **camera**: 1. Keep …

☆ 99 Cited by 114 Related articles All 11 versions »

Quantifying and **recognizing** human **movement** patterns from monocular video images-part ii: applications to **biometrics**

RD Green, L Guan - IEEE Transactions on Circuits and Systems …, 2004 - ieeexplore.ieee.org

… [11] R. Green, L. Guan, and JA Burne, "Real-time gait analysis for diag- nosing **movement** disorders," J … [20] I. Mikic, M. Triverdi, E. Hunter, and P. Cosman, "Articulated body pos- ture estimation from multi-**camera** voxel data … [22] H. Murase and R. Sakai, "**Moving** object **recognition** …

☆ 99 Cited by 54 Related articles All 14 versions

Multiple **camera** tracking of interacting and occluded human motion

SL Dockstader, AM Tekalp - Proceedings of the IEEE, 2001 - ieeexplore.ieee.org

… The system is composed of multiple tasks including **position detection**, rotation angle **detection** and body-side … when the active **camera** no longer has a sufficient view of the **moving** object. Selecting the optimal **camera** is based on a matching evaluation, which uses a simple …

☆ 99 Cited by 260 Related articles All 11 versions

Live **face detection** based on the analysis of fourier spectra

J Li, Y Wang, T Tan, AK Jain - Proc. of SPIE Vol, 2004 - proceedings.spiedigitallibrary.org

... Using structure and **movement** information of live **face**, an effective live **face detection** algorithm is ... This is because big size photo has more **facial** details to fool the system ... as faces are located very well, frequency dynamic descriptors can easily determine the liveness of the **face** ...

☆ 99 Cited by 256 Related articles All 11 versions

Local binary patterns as an image preprocessing for **face authentication**

G Heusch, Y Rodriguez, S Marcel - ... and Gesture Recognition ..., 2006 - ieeexplore.ieee.org

... An image preprocessing al- gorithm for illumination invariant **face recognition**. In Audio- and Video-Based **Biometric** Person Authentica- tion, AVBPA'03, 2003 ... A texture- based method for detecting **moving** objects ... **Face detection** using improved LBP under bayesian framework ...

☆ 99 Cited by 211 Related articles All 21 versions »

Liveness **detection** for **face recognition**

G Pan, Z Wu, L Sun - Recent advances in face recognition, 2008 - intechopen.com

... Head **movement** High No Middle Eye blinking Low No Low ... Combining with the **facial** localization system, the whole system could achieve an online processing speed of nearly 20fps, which is reasonable for practical applications ... Liveness **Detection** for **Face Recognition** 121 ...

☆ 99 Cited by 114 Related articles All 11 versions »

Moving face spoofing **detection** via 3D projective invariants

M De Marsico, M Nappi, D Riccio... - Biometrics (ICB), 2012 ..., 2012 - ieeexplore.ieee.org

... With a fast **movement**, the cross ratio rapidly changes providing a higher variance ... 3, pp. 303–331, 2005. [9] J. Li, Y. Wang, T. Tan, A. Jain, Live **Face Detection** Based on ... SPIE, vol. 5404, pp. 296–303, 2004. [10] S. Milborrow. Locating **Facial** Features with Active Shape Models ...

☆ 99 Cited by 68 Related articles All 5 versions »

Motion-based counter-measures to photo attacks in **face recognition**

A Anjos, MM Chakka, S Marcel - IET biometrics, 2013 - IET

... at the **face** centre; 3. Define three bounding boxes surrounding the **face** centre and ear centres; 4. If the head is **moving** more horizontally ... Our proposed algorithm measures motion correlation between **face** and background solely using the **movement** direction ...

☆ 99 Cited by 52 Related articles All 11 versions

Continuous video monitoring using **face recognition** for access control

JJ Atick, PA Griffin, AN Redlich - US Patent 6,111,517, 2000 - Google Patents

... and 625 the system searches the field of view for any **movement**, rather than ... US5835616 *, Jun 17, 1994, Nov 10, 1998, University Of Central Florida, **Face detection** using templates. US5991429 *, Dec 6, 1996, Nov 23, 1999, Coffin; Jeffrey S. **Facial recognition** system for security ...

☆ 99 Cited by 225 Related articles All 2 versions

Three-dimensional imaging system for pattern **recognition**

CS Seo, GI Cho - US Patent 7,212,330, 2007 - Google Patents

... **face recognition** systems is the acquisition of three-dimensional images for both **facial** database and ... field of view and the optical axis are adjusted without the macroscopic **movement** of the ... Patrick Flynn, "A Survey Of 3D and Multi-Modal 3D+2D **Face Recognition**," Notre Dame ...

☆ 99 Cited by 33 Related articles All 4 versions

Iris **recognition**: The **path** forward

A Ross - Computer, 2010 - ieeexplore.ieee.org

... based multibiometric systems that can operate in environments characterized by harsh lighting, **moving** subjects, and ... ocular features with local **facial** attributes such as skin texture and **facial** marks in the periocular region can enhance the performance of **face**-based **biometric** ...

☆ 99 Cited by 119 Related articles All 14 versions

Face recognition using 2D and 3D **facial** data

K Chang, K Bowyer, P Flynn - ... User **Authentication**, 2003 - pdfs.semanticscholar.org

... The accu- racy requirement might be vary under different conditions of subjects, such as **facial** muscle **movement**, or imaging condition changes ... [17] Y. Wang, C. Chua, and Y. Ho, "**Facial** feature **detection** and **face recognition** from 2D and 3D images," Pattern Recogni-

☆ 99 Cited by 384 Related articles All 12 versions »

Face recognition system and method therefor

H Wisniewski - US Patent App. 10/622,512, 2003 - Google Patents

... To generate the database for **facial** searching, or to create an identification card, enrollment can ... as **moving** the head to various angles, and preventing certain eye **movement** such as ... To ensure a fair comparison of images, the program of the present **face recognition** system puts ...

☆ 99 Cited by 45 Related articles All 2 versions

U.S. Patent and Trademark Office

SIGN IN SIGN UP
(+authentication +biometric +fac

Searched for *(+authentication +biometric +facial +recognition +expected +movement +parameter)* [new search] [edit/save query] [advanced search]

Searched The ACM Full-Text Collection: 483,622 records [Expand your search to The ACM Guide to Computing Literature: 2,725,384 records]

0 results found

Nothing found

The ACM Digital Library is published by the Association for Computing Machinery. Copyright © 2017 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

IEEE.org | IEEE *Xplore* Digital Library | IEEE-SA | IEEE Spectrum | More Sites Cart (0) | Create Account | Personal Sign In

Access provided by:
United States Patent and Trademark Office
Sign Out

Browse My Settings Get Help

Search within results Show: All Results | Per Page: 25 | Download PDFs | Export | Set Search Alerts | Search History

Displaying results **1-25** of **35** for
(((((("Abstract":biometric) AND facial recognition) AND expected movement) AND parameter) AND authentication) enrollment
and refined by
Year: 1999-2014

☐ Conference Publications (20) ☐ Journals & Magazines (14) ☐ Books & eBooks (1)

Year

Single Year | Range

☐ 1999 ☐ 2014

From 1999 To 2014

Author

Affiliation

Publication Title

Publisher

Supplemental Items

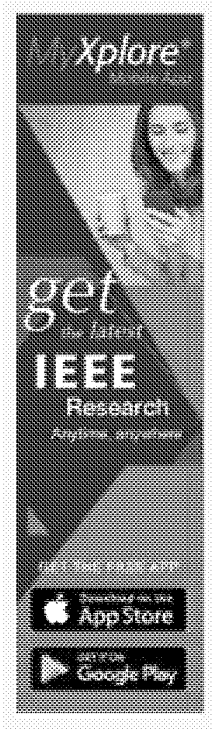
Conference Location

☐ **Biometric security technology**
M. Faundez-Zanuy
IEEE Aerospace and Electronic Systems Magazine
Year: 2006, Volume: 21, Issue: 6
Pages: 15 - 26
Cited by: Papers (33) | Patents (2)
IEEE Journals & Magazines
Abstract (2828 Kb)

☐ **Person identification using behavioral features from lip motion**
Usman Saeed
Face and Gesture 2011
Year: 2011
Pages: 131 - 136
IEEE Conference Publications
Abstract (210 Kb)

☐ **Using Haptic Interfaces for User Verification in Virtual Environments**
Mauricio Orozco; Matthew Graydon; Shervin Shirmohammadi; Abdulmotaleb El Saddik
2006 IEEE Symposium on Virtual Environments, Human-Computer Interfaces and Measurement Systems
Year: 2006
Pages: 25 - 30
Cited by: Papers (5) | Patents (3)
IEEE Conference Publications
Abstract (280 Kb)

☐ **Complex Eye Movement Pattern Biometrics: The Effects of Environment and Stimulus**
Corey D. Holland; Oleg V. Komogortsev
IEEE Transactions on Information Forensics and Security
Year: 2013, Volume: 8, Issue: 12
Pages: 2115 - 2126
Referenced in: IEEE Biometrics Compendium, IEEE RFID Virtual Journal, IEEE RFID Virtual Journal
Cited by: Papers (14)
IEEE Journals & Magazines



☐ **Biometric Antispoofing Methods: A Survey in Face Recognition**
Javier Galbally; Sébastien Marcel; Julian Fierrez
IEEE Access
Year: 2014, Volume: 2
Pages: 1530 - 1552
Cited by: Papers (19)
IEEE Journals & Magazines

Abstract (10682 Kb)

☐ **Periocular Biometrics in the Visible Spectrum**
Unsang Park; Raghavender Reddy Jillela; Arun Ross; Anil K. Jain
IEEE Transactions on Information Forensics and Security
Year: 2011, Volume: 6, Issue: 1
Pages: 96 - 106
Referenced in: IEEE Biometrics Compendium, IEEE RFIC Virtual Journal, IEEE RFID Virtual Journal
Cited by: Papers (95)
IEEE Journals & Magazines

Abstract (1190 Kb)

☐ **Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication**
Mario Frank; Ralf Biedert; Eugene Ma; Ivan Martinovic; Dawn Song
IEEE Transactions on Information Forensics and Security
Year: 2013, Volume: 8, Issue: 1
Pages: 136 - 148
Referenced in: IEEE Biometrics Compendium, IEEE RFIC Virtual Journal, IEEE RFID Virtual Journal
Cited by: Papers (125) | Patents (5)
IEEE Journals & Magazines

Abstract (1709 Kb)

☐ **On Continuous User Authentication via Typing Behavior**
Joseph Roth, Xiaoming Liu; Dimitris Metaxas
IEEE Transactions on Image Processing
Year: 2014, Volume: 23, Issue: 10
Pages: 4611 - 4624
Cited by: Papers (14)
IEEE Journals & Magazines

Abstract (3739 Kb) Media

☐ **FAME: Face Authentication for Mobile Encounter**
Silvio Barra; Maria De Marsico; Chiara Galdi; Daniel Riccio; Harry Wechsler
2013 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications
Year: 2013
Pages: 1 - 7
Cited by: Papers (2)
IEEE Conference Publications

Abstract (581 Kb)

« First < 1 2 > Last »

IEEE Account
» Change Username/Password

Purchase Details
» Payment Options

Profile Information
» Communications Preferences

Need Help?
» **US & Canada:** +1 800 678 4333

› Update Address › Order History › Profession and Education › Worldwide: +1 732 981 0060
› View Purchased Documents › Technical Interests › Contact & Support

About IEEE *Xplore* | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.
© Copyright 2017 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

ACM DIGITAL LIBRARY U.S. Patent and Trademark Office

SIGN IN SIGN UP

recordAbstract:(identity authentic

Searched for *recordAbstract:(identity authentication biometric +movement) AND (+path +parameter +expected display image)* [new search] [edit/save query] [advanced search]

Searched The ACM Full-Text Collection: 483,622 records [Expand your search to The ACM Guide to Computing Literature: 2,725,384 records]

1 results found Export Results: bibtex | endnote | acmref | csv

Refine by People
Names
Institutions
Authors

Refine by Publications
Publication Names
ACM Publications
All Publications
Content Formats
Publishers

Refine by Conferences
Sponsors

Result 1 – 1 of 1 Sort by: relevance

1 A compact normal walk model for PCS networks

Chiu-Ching Tuan, Chen-Chau Yang

October 2003 ACM SIGMOBILE Mobile Computing and Communications Review: Volume 7 Issue 4, October 2003

Publisher: ACM

Bibliometrics: Citation Count: 1
Downloads (6 Weeks): 3, Downloads (12 Months): 4, Downloads (Overall): 299

Full text available: Pdf

Model-based movement patterns play a crucial role in evaluating the performance of mobility-dependent Personal Communication Service (PCS) strategies. This study proposes a new normal walk model to represent more closely the daily movement patterns of a mobile station (MS) in PCS networks than a conventional random walk model. The proposed ...

[result highlights]

Result 1 – 1 of 1

The ACM Digital Library is published by the Association for Computing Machinery. Copyright © 2017 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

IEEE.org | IEEE *Xplore* Digital Library | IEEE-SA | IEEE Spectrum | More Sites Cart (0) | Create Account | Personal Sign In

Access provided by:
United States Patent and Trademark Office
Sign Out

Browse My Settings Get Help

Search within results Show: All Results | Download PDFs | Export | Set Search Alerts | Search History

Displaying results 1-8 of 8 for

((((("Abstract":authentication biometric) AND facial recognition) AND path parameter) AND enrolled) AND image) and refined by

Year: 1990-2014

Conference Publications (4) Journals & Magazines (4)

Year

Single Year | Range

1997 2014

From To

1997 2014

Author

Affiliation

Publication Title

Publisher

Conference Location

The role of geometry in age estimation
Pavan Turaga; Soma Biswas; Rama Chellappa
2010 IEEE International Conference on Acoustics, Speech and Signal Processing
Year: 2010
Pages: 946 - 949
Cited by: Papers (10)
IEEE Conference Publications

Abstract (269 Kb)

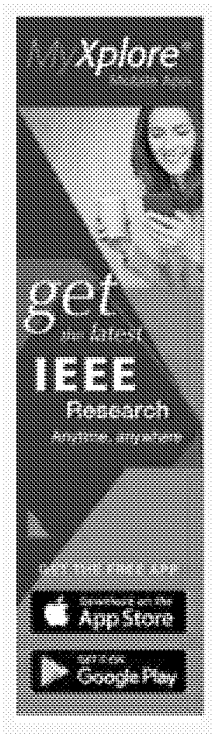
An identity-authentication system using fingerprints
A. K. Jain; Lin Hong; S. Pankanti; R. Bolle
Proceedings of the IEEE
Year: 1997, Volume: 85, Issue: 9
Pages: 1365 - 1388
Cited by: Papers (380) | Patents (26)
IEEE Journals & Magazines

Abstract (704 Kb)

Enhancing security and privacy in biometrics-based authentication systems
N. K. Ratha; J. H. Connell; R. M. Bolle
IBM Systems Journal
Year: 2001, Volume: 40, Issue: 3
Pages: 614 - 634
Cited by: Papers (275) | Patents (81)
IBM Journals & Magazines

Abstract (3787 Kb)

Systematic Error Analysis for the Enhancement of Biometric Systems Using Soft Biometrics
Anastasios Drosou; Dimitrios Tzovaras; Konstantinos Moustakas; Maria Petrou
IEEE Signal Processing Letters
Year: 2012, Volume: 19, Issue: 12
Pages: 833 - 836
Referenced in: IEEE Biometrics Compendium, IEEE RFIC Virtual Journal, IEEE RFID Virtual Journal
Cited by: Papers (1)
IEEE Journals & Magazines



IEEE Conference Publications

Abstract (821 Kb)

☐ **Unobtrusive multi-modal biometric recognition using activity-related signatures**
A. Drosou; G. Stavropoulos; D. Ioannidis; K. Moustakas; D. Tzovaras
IET Computer Vision
Year: 2011, Volume: 5, Issue: 6
Pages: 367 - 379
IET Journals & Magazines

Abstract (967 Kb)

☐ **A binary tree authentication scheme based on multi-biometrics**
Qi Deng; Qiuyun Lv; Qiuhua Wang
ICINS 2014 - 2014 International Conference on Information and Network Security
Year: 2014
Pages: 115 - 120
IET Conference Publications

Abstract (646 Kb)

☐ **Biometric recognition in telecom environment**
Ivan Krevatin
2010 14th International Conference on Intelligence in Next Generation Networks
Year: 2010
Pages: 1 - 6
IEEE Conference Publications

Abstract (195 Kb)

« First < 1 > Last »

IEEE Account	Purchase Details	Profile Information	Need Help?
» Change Username/Password	» Payment Options	» Communications Preferences	» **US & Canada:** +1 800 678 4333
» Update Address	» Order History	» Profession and Education	» **Worldwide:** +1 732 981 0060
	» View Purchased Documents	» Technical Interests	» Contact & Support

About IEEE *Xplore* | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.
© Copyright 2017 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

IEEE.org | IEEE *Xplore* Digital Library | IEEE-SA | IEEE Spectrum | More Sites Cart (0) | Create Account | Personal Sign In

Access provided by:
United States Patent and Trademark Office
Sign Out

Browse My Settings Get Help

Search within results Show: All Results | Download PDFs | Export | Set Search Alerts | Search History

Displaying results 1-9 of 9 for

((((((("Abstract":biometric) AND facial recognition) AND path parameter) AND registered) AND image) AND expected) AND identity)

display

and refined by

Year: 1990-2014

Journals & Magazines (7) Conference Publications (2)

Year

Single Year | Range

1997 2014

From To

1997 2014

Author

Affiliation

Publication Title

Conference Location

Gait recognition: a challenging signal processing technology for biometric identification
N. V. Boulgouris; D. Hatzinakos; K. N. Plataniotis
IEEE Signal Processing Magazine
Year: 2005, Volume: 22, Issue: 6
Pages: 78 - 90
Cited by: Papers (133)
IEEE Journals & Magazines

Abstract (946 Kb)

Using Haptic Interfaces for User Verification in Virtual Environments
Mauricio Orozco; Matthew Graydon; Shervin Shirmohammadi; Abdulmotaleb El Saddik
2006 IEEE Symposium on Virtual Environments, Human-Computer Interfaces and Measurement Systems
Year: 2006
Pages: 25 - 30
Cited by: Papers (5) | Patents (3)
IEEE Conference Publications

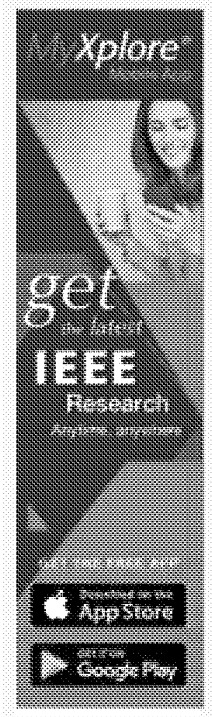
Abstract (280 Kb)

Biometric Antispoofing Methods: A Survey in Face Recognition
Javier Galbally; Sébastien Marcel; Julian Fierrez
IEEE Access
Year: 2014, Volume: 2
Pages: 1530 - 1552
Cited by: Papers (19)
IEEE Journals & Magazines

Abstract (10682 Kb)

An identity-authentication system using fingerprints
A. K. Jain; Lin Hong; S. Pankanti; R. Bolle
Proceedings of the IEEE
Year: 1997, Volume: 85, Issue: 9
Pages: 1365 - 1388
Cited by: Papers (380) | Patents (26)
IEEE Journals & Magazines

Abstract (704 Kb)



Abstract

Systematic Error Analysis for the Enhancement of Biometric Systems Using Soft Biometrics
Anastasios Drosou, Dimitrios Tzovaras, Konstantinos Moustakas, Maria Petrou
IEEE Signal Processing Letters
Year: 2012, Volume: 19, Issue: 12
Pages: 833 - 836
Referenced in: IEEE Biometrics Compendium, IEEE RFIC Virtual Journal, IEEE RFID Virtual Journal
Cited by: Papers (1)
IEEE Journals & Magazines

Abstract (741 Kb)

Assessing the Uniqueness and Permanence of Facial Actions for Use in Biometric Applications
Lanthao Benedikt; Darren Cosker; Paul L. Rosin; David Marshall
IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans
Year: 2010, Volume: 40, Issue: 3
Pages: 449 - 460
Referenced in: IEEE Biometrics Compendium, IEEE RFIC Virtual Journal, IEEE RFID Virtual Journal
Cited by: Papers (19)
IEEE Journals & Magazines

Abstract (1930 Kb)

Face Recognition by Super-Resolved 3D Models From Consumer Depth Cameras
Stefano Berretti; Pietro Pala; Alberto del Bimbo
IEEE Transactions on Information Forensics and Security
Year: 2014, Volume: 9, Issue: 9
Pages: 1436 - 1449
Referenced in: IEEE Biometrics Compendium, IEEE RFIC Virtual Journal, IEEE RFID Virtual Journal
Cited by: Papers (6)
IEEE Journals & Magazines

Abstract (8713 Kb)

Biometric recognition in telecom environment
Ivan Krevatin
2010 14th International Conference on Intelligence in Next Generation Networks
Year: 2010
Pages: 1 - 6
IEEE Conference Publications

Abstract (185 Kb)

« First < 1 > Last »

IEEE Account
» Change Username/Password
» Update Address

Purchase Details
» Payment Options
» Order History
» View Purchased Documents

Profile Information
» Communications Preferences
» Profession and Education
» Technical Interests

Need Help?
» **US & Canada:** +1 800 678 4333
» **Worldwide:** +1 732 981 0060
» Contact & Support

About IEEE *Xplore* | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.
© Copyright 2017 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		5,031,228	07/91	Lu			
		5,699,449	12/97	Javidi			
		5,784,056	07/98	Nielsen			
		5,835,616	11/98	Lobo, et al.			
		6,212,030	07/91	Lu			
		6,461,807	12/97	Javidi			
		6,961,361	11/98	Lobo, et al.			
		7,211,138	07/91	Lu			
		7,460,916	12/97	Javidi			
		7,710,693	07/98	Nielsen			
		7,960,470	11/98	Lobo, et al.			
		8,210,247	07/91	Lu			
		8,460,024	12/97	Javidi			
		8,709,801	07/98	Nielsen			
		8,959,578	11/98	Lobo, et al.			
		9,209,355	07/91	Lu			
		9,459,132	12/97	Javidi			
		9,708,909	07/98	Nielsen			
		9,958,687	11/98	Lobo, et al.			
		10,208,464	07/91	Lu			
		10,458,241	12/97	Javidi			
		10,957,795	11/98	Lobo, et al.			
		11,207,572	07/91	Lu			
		11,457,349	12/97	Javidi			
		5,031,228	07/91	Lu			
		5,699,449	12/97	Javidi			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/06/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2003/0236832	12/03	McIntyre, et al.			
		6,678,664	01/04	Ganesan			
		6,687,390	02/04	Avni			
		6,697,502	02/04	Luo			
		6,728,401	04/04	Hardeberg			
		2004/0070678	04/04	Toyama, et al.			
		2004/0081338	04/04	Takenaka			
		2004/0125991	07/04	Yokoi			
		2004/0143598	07/04	Drucker, et al.			
		6,775,397	08/04	Hamalainen			
		2004/0190758	09/04	Doi, et al.			
		2004/0109584	10/04	Lestideau			
		2004/0201709	10/04	McIntyre, et al.			
		6,840,149	10/04	Squilla, et al.			
		20047/0264780	12/04	Zhang, et al.			
		2005/0031173	02/05	Hwang			
		2005/0065855	03/05	Geller			
		2005/0094849	05/05	Sung, et al.			
		2005/0100195	05/05	Li			
		2005/0117802	06/05	Yonaha, et al.			
		2005/0141766	06/05	Nagahashi, et al.			
		2005/0180627	08/05	Yang, et al.			
		2005/0190273	09/05	Toyama, et al.			
		2005/0220347	10/05	Enomoto			
		2005/0251015	11/05	Takikawa, et al.			
		2005/0265603	12/05	Porter, et al.			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/06/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		7,003,135	02/06	Hsieh, et al.			
		2006/0050933	03/06	Adam, et al.			
		2006/0110014	05/06	Philomin			
		2006/0133672	06/06	Li			
		2006/0156029	07/06	Algazi			
		2006/0173560	08/06	Widrow			
		2006/0218225	09/06	Hee Voon, et al.			
		2006/0222215	10/06	Jung, et al.			
		2006/0239515	10/06	Zhang, et al.			
		2006/0251292	11/06	Gokturk, et al.			
		2006/0251338	11/06	Gokturk, et al.			
		2006/0251339	11/06	Gokturk, et al.			
		2006/0253491	11/06	Gokturk, et al.			
		2006/0274978	12/06	Fukuda, et al.			
		2007/0074114	03/07	Adjali			
		2007/0081744	04/07	Gokturk, et al.			
		2007/0098303	05/07	Gallagher, et al.			
		7,218,774	05/07	Liu			
		7,231,657	06/07	Honarvar			
		2007/177805	08/07	Gallagher			
		2007/0206834	09/07	Shinkai, et al.			
		2007/0211925	09/07	Aoki, et al.			
		7,289,648	10/07	Liu			
		7,308,581	12/07	Geosimonian			
		7,333,963	02/08	Widrow, et al.			
		2008/0046458	02/08	Tseng, et al.			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/06/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2008/077595	03/08	Leebow			
		2008/0080743	04/08	Schneiderman, et al.			
		2008/0080745	04/08	Vanhoucke, et al.			
		2008/0091723	04/08	Zuckerberg, et al.			
		2008/0130960	06/08	Yagnik			
		7,415,152	08/08	Jiang, et al.			
		2008/0212849	09/08	Gao			
		2008/317379	12/08	Steinberg, et al.			
		7,519,200	04/09	Gokturk, et al.			
		2009/0185784	07/09	Hiroike, et al.			
		2009/0226052	09/09	Fedel			
		2009/232367	09/09	Shinzaki			
		2009/0252383	10/09	Adam, et al.			
		7,636,450	12/09	Bourdev			
		2009/0324018	12/09	Tell			
		2009/0324022	12/09	Sangberg, et al.			
		2009/0324137	12/09	Stallings, et al.			
		7,646,909	01/10	Jiang, et al.			
		7,660,444	02/10	Hamalainen			
		2010/0050134	02/10	Clarkson			
		20,100,067,750	03/10	Matsuo			
		2010/0054600	03/10	Anbalagan, et al.			
		2010/0054601	03/10	Anbalagan, et al.			
		2010/0061631	03/10	Omori			
		2010/0158327	06/10	Kangas, et al.			
		7,788,247	08/10	Wang, et al.			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/06/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2010/0232656	09/10	Ryu			
		7,804,982	09/10	Howard, et al.			
		2010/245614	09/10	Matsunaga			
		7,809,722	10/10	Gokturk, et al.			
		2010/272363	10/10	Steinberg, et al.			
		2010/0287053	11/10	Ganong, et al.			
		2010/0318366	12/10	Sullivan			
		2010/0317420	12/10	Hoffberg			
		2,011,063,108	03/11	Aonuma, et al.			
		7,945,653	05/11	Zuckerberg, et al.			
		2011/0169853	07/11	Oiwa			
		2011/0202531	08/11	Zuckerberg, et al.			
		2011/0225481	09/11	Zuckerberg, et al.			
		2011/0282906	11/11	Wong			
		D650,793	12/11	Impas			
		8,121,408	02/12	Omori			
		8,165,352	04/12	Mohanty, et al.			
		8,244,211	08/12	Clark			
		D667,423	09/12	Nagamine			
		8,316,237	11/12	Felsher, et al.			
		2012/0323704	12/12	Steelberg			
		8,326,000	12/12	Jung, et al.			
		2013/0007032	01/13	Klappert			
		2013/0066526	03/13	Mondragon			
		8,392,268	03/13	Smith, et al.			
		2013/057693	03/13	Baranek			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/06/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		8,396,246	03/13	Anbalagan, et al.			
		2013/077835	03/13	Kritt, et al.			
		8,416,312	04/13	Matsunaga			
		2013/0179298	07/13	Segman			
		2013/0226740	08/13	Biliosa			
		2013/0246158	09/13	Cannon			
		2013/0267204	10/13	Schultz			
		2013/0342672	12/13	Gray, et al.			
		2014/0012756	01/14	Beraja			
		2014/0059673	02/14	Azar			
		8,649,604	02/14	Steinberg, et al.			
		214/0098174	04/14	Summers			
		2014/0118257	05/14	Baldwin			
		2014/0165187	06/14	Daesung			
		2014/0169643	06/14	Todoroki			
		8,743,051	06/14	Moy, et al.			
		8,750,574	06/14	Ganong, et al.			
		2014/0198959	07/14	Derakhshani			
		8,788,977	07/14	Bezos			
		8,856,541	10/14	Chaudhury			
		8,867,849	10/14	Kirkham			
		2014/0337948	11/14	Hoyos			
		8,922,480	12/14	Freed, et al.			
		2015/0052462	02/15	Kulkarni			
		2015/0055821	02/15	Fotland			
		2015/0077323	03/15	Ramaswamy			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/06/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		D726,221	04/15	Gomez			
		9,037,354	05/15	Mondragon			
		2015/0131872	05/15	Ganong, et al.			
		2015/0153571	06/15	Ballard			
		9,076,028	07/15	Summers			
		9,076,008	07/15	Moy			
		D737,325	08/15	Kim			
		9,137,246	09/15	Parry, et al.			
		2015/0310260	10/15	Summers			
		9,152,849	10/15	Ganong, et al.			
		9,202,105	12/15	Wang, et al.			
		2015/0378433	12/15	Savastinuk			
		2016/0063235	03/16	Tussy			
		D753,132	04/16	Cuthbert			
		D756,401	05/16	Soldner			
		2016/0209939	07/16	Zambetti			
		9,424,491	08/16	Kirkham			
		9,430,695	08/16	Summers			
		D762,655	08/16	Kai			
		D762,673	08/16	Seo			
		D762,715	08/16	Williamson			
		D763,271	08/16	Everette			
		2016/0259528	09/16	Foss			
		2016/0261675	09/16	Block			
		D765,674	09/16	Kim			
		D769,933	10/16	Sabia			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/06/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2016/0342826	11/16	Apostolos, et al.			
		D776,680	01/17	Bae			
		D778,923	02/17	Zhou			
		D778,940	02/17	Williamson			
		9,607,138	03/17	Baldwin			
		D780,781	03/17	Ding			
		9,600,649	03/17	Parry, et al.			
		D783,633	04/17	Oh			
		D783,652	04/17	Guan			
		D784,363	04/17	Fleming			
		D787,527	05/17	Wilberding			
		D788,122	05/17	Tada			
		9,740,848	08/17	Parry, et al.			
		2017/0220843	08/17	Apostolos, et al.			

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
							YES	NO
		EP 1388802	02/04	Europe			X	
		EP 1455297	09/04	Europe			X	
		WO 2006/130542	12/06	WIPO			X	
		WO 2008/107002	09/08	WIPO			X	
		WO 2015/070320	05/15	WIPO			X	

EXAMINER INITIAL		**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)
		After Effects Tutorial - 17 - Introduction to Masking, by thenewboston, uploaded 12/07/2008, youtube.com [online], [retrieved 06/15/2017]. Available from <URL:https://www.youtube.com/watch?v=kWd51xDqzIc>

EXAMINER	/SHANTO ABEDIN/	DATE CONSIDERED	12/06/2017

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

EXAMINER INITIAL		**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)
		Optical Illusions - Animated GIF & JPG, dated 10/28/2013, plus.google.com [online], [retrieved 06/19/2017]. Available from internet <URL:https://plus.google.com/+Whak-Off/posts/CX4YhzXSQy2>
		The Universal Face Login for 5 Billion Smartphones, zoomlogin.com [online], [retrieved 06/19/2017]. Available from internet <URL:https://zoomlogin.com/>
		Wong, Yongkang, et al. "Patch-based probabilistic image quality assessment for face selection and improved video-based face recognition." CVPR 2011 WORKSHOPS. IEEE, 2011
		RAFALOVITCH, "Viewfinder Friends-idea for Facebook application", November 14, 2007, http://blog.outerthoughts.com/2007/11/viewfinder-friends-idea-for-facebook-application/, 5pages.
		KISHORE, "How to Add, Upload, and Tag Your Pictures and Photos in FaceBook", http://www.online-tech-tips.com/fun-stuff/how-to-add-upload-and-tag-your-pictures-and-photos-in-facebook/, August 11, 2007, 13 pages.
		BECKER et al., "Evaluation of Face Recognition Techniques for Application to Facebook", IEEE International conference on Automatic Face and Gesture Recognition, 2008, 6 pages.
		BAKER, "Google & Riya Face Recognition Photo Search", November 22, 2005, http://www.searchenginejournal.com/google-riya-face-recognition-photo-search/25501, 1 page_
		PONCE, "Riya, Photo Sharing with Face Recognition", October 28, 2005, http://www.ohgizmo.com/2005/10/28/riya-photo-sharing-with-face-recognition/, 2 pages_
		FACEBOOK, "Making Photo Tagging Easier", https://m.facebook.com/notes/facebook/making-photo-tagging-easier/467145887130/?_tn_=C&_rdr, 2 pages
		MICHELSON et al., "Auto-tagging the Facebook", 2006, http://cs229.stanford.edu/proj2006/MichelsonOrtiz-AutoTaggingTheFacebook.pdf, 5 pages.
		ARRINGTON, "First Screen Shots of Riya", October 26, 2005, http://techcrunch.com/2005/10/26/riya-prepares-to-launch-alpha/, 10 pages
		ARRINGTON, "Ojos - Auto Name & Tag Your Photos", August 15, 2005, http://techcrunch.com/2005/08/31/ojos-auto-name-tag-your-photos/, 8 pages.
		STONE, et al. "Autotagging Facebook: Social network context improves photo annotation," In Workshop on Internet Vision, 2008, 2 pages_ ALL R
		SCHUON et al., "CS229 Project Report: Automated photo tagging in Facebook", December 2007, http://cs229.Stanford.edu/proj2007/SchuonRobertsonZou-AutomatedPhotoTaggingInFacebook.pdf, 5 pages.
		YADAV, "Facebook - The Complete Biography", August 25, 2006, http://mashable.com12006/08/25/facebook-protile/, 7 pages_
		UNKNOWN, "What does it mean to "tag" someones picture on facebook, whats the point of doing it?", November 28, 2007, https://answers.yahoo.com/question/index?qid=20071128123629AAY0DLP, 2 pages.
		Yang, et al., "Detecting Faces in Images: A Survey", January 2002, IEEE Trans. Pattern Analysis Machine Intelligence, 24(1), 2 pages

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 12/06/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 6236

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/839,505	08/28/2015 RULE	726	2436	FACIAL.0012P

APPLICANTS

INVENTORS

Kevin Alan Tussy, Las Vegas, NV;

**** CONTINUING DATA ***************************

This appln claims benefit of 62/043,224 08/28/2014

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **

09/11/2015

Foreign Priority claimed	❑ Yes ☑ No	❑ Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
35 USC 119(a-d) conditions met	❑ Yes ❑ No					
Verified and Acknowledged	/SHANTO ABEDIN/ Examiner's Signature	Initials	NV	14	21	3

ADDRESS

WEIDE & MILLER, LTD.
10655 Park Run Drive
SUITE 100
LAS VEGAS, NV 89144
UNITED STATES

TITLE

Facial Recognition Authentication System Including Path Parameters

FILING FEE RECEIVED		
770	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	❑ All Fees ❑ 1.16 Fees (Filing) ❑ 1.17 Fees (Processing Ext. of time) ❑ 1.18 Fees (Issue) ❑ Other _____ ❑ Credit

BIB (Rev. 05/07).

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14839505	TUSSY, KEVIN ALAN
	Examiner	**Art Unit**
	SHANTO M ABEDIN	2436

CPC						
Symbol					**Type**	**Version**
G06F		21	/	32	F	2013-01-01
G06F		21	/	34	I	2013-01-01
G06Q		20	/	3276	I	2013-01-01
G06K		9	/	00255	I	2013-01-01
G06Q		20	/	40145	I	2013-01-01
G06K		9	/	00912	I	2013-01-01
G06K		9	/	00926	I	2013-01-01
G06K		9	/	22	I	2013-01-01
			/			
			/			
			/			
			/			
			/			
			/			
			/			

CPC Combination Sets							
Symbol				**Type**	**Set**	**Ranking**	**Version**
			/				
			/				

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	20	
/SHANTO M ABEDIN/ Primary Examiner.Art Unit 2436	12/06/2017	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No. 20171206

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14839505	TUSSY, KEVIN ALAN
	Examiner	**Art Unit**
	SHANTO M ABEDIN	2436

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
726	6	G	0	6	F	21 / 32 (2013.01.01)						
CROSS REFERENCE(S)		G	0	6	F	21 / 34 (2013.01.01)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)											

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	20	
/SHANTO M ABEDIN/ Primary Examiner.Art Unit 2436	12/06/2017	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No. 20171206

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14839505	TUSSY, KEVIN ALAN
	Examiner	**Art Unit**
	SHANTO M ABEDIN	2436

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1		17												
2	2		18												
3	3		19												
4	4		20												
5	5		21												
6	6	15	22												
7	7	16	23												
8	8	17	24												
9	9	18	25												
10	10	19	26												
11	11	20	27												
12	12														
13	13														
14	14														
	15														
	16														

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 20	
/SHANTO M ABEDIN/ Primary Examiner.Art Unit 2436 (Primary Examiner)	12/06/2017 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

U.S. Patent and Trademark Office Part of Paper No. 20171206

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14839505	TUSSY, KEVIN ALAN
	Examiner	**Art Unit**
	SHANTO M ABEDIN	2436

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	07/10/2017	12/06/2017							
1	1	✓	=							
2	2	✓	=							
3	3	✓	=							
4	4	✓	=							
5	5	✓	=							
6	6	✓	=							
7	7	✓	=							
8	8	O	=							
9	9	✓	=							
10	10	✓	=							
11	11	✓	=							
12	12	✓	=							
13	13	✓	=							
14	14	✓	=							
	15	✓	-							
	16	✓	-							
	17	✓	-							
	18	✓	-							
	19	✓	-							
	20	✓	-							
	21	✓	-							
15	22		=							
16	23		=							
17	24		=							
18	25		=							
19	26		=							
20	27		=							

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1948	(movement)same(camera)same(user)same(path)	US-PGPUB; USPAT	AND	ON	2017/11/16 12:34
L3	60454	(movement or path)same(camera or mobile)same(user or path)same(sequential$4 or compar$4 or determin$4)	US-PGPUB; USPAT	AND	ON	2017/11/16 12:35
L4	62557	(movement or path)same(camera or mobile)same(user or path or parameter)same(sequential$4 or compar$4 or determin$4)	US-PGPUB; USPAT	AND	ON	2017/11/16 12:35
L5	6425	(movement or moving)same(camera)same(user or hand)same(path or parameter)	US-PGPUB; USPAT	AND	ON	2017/11/16 12:36
L7	65522	L4 OR L5	US-PGPUB; USPAT	AND	ON	2017/11/16 12:36
L8	15310	L7(movement or moving or path or direction)same(camera or mobile or smartphone)same(user or hand or particular or expected)same(path or parameter or direction or area or display)(authenticat$4 or identity)	US-PGPUB; USPAT	AND	ON	2017/11/16 12:37
L9	10719	L8(authenticat$4 or identity)(camera)	US-PGPUB; USPAT	AND	ON	2017/11/16 12:38
L11	6753	L8(authenticat$4 or identity)(camera)(threshold)	US-PGPUB; USPAT	AND	ON	2017/11/16 12:38
L12	7917	L8(authenticat$4 or identity)(camera)(threshold or meet$4)	US-PGPUB; USPAT	AND	ON	2017/11/16 12:39
L13	559	L12(movement or moving or path or direction)near5(camera or mobile or smartphone)same(user or hand or particular or expected or head or face)same(path or parameter or direction or area or display or sequential$4 or predetermined)(authenticat$4 or identity).clm.	US-PGPUB; USPAT	AND	ON	2017/11/16 12:40
L14	72	L12(movement or moving or path or direction)near5(camera or mobile or smartphone)same(user or hand or particular or expected or head or face or determin$4)same(path or parameter or direction or area or display or sequential$4 or predetermined).clm.(authenticat$4 or identity or enroll$5 or register$4).clm.	US-PGPUB; USPAT	AND	ON	2017/11/16 12:41
L15	567	L13 OR L14	US-PGPUB; USPAT	AND	ON	2017/11/16 12:41
L16	489	L15(movement or moving)(path or direction)	US-PGPUB; USPAT	AND	ON	2017/11/16 12:41
L17	335	L15(movement or moving)(path or direction)(camera)(authenticat$4 or identity)(register$4 or enroll$4 or enrollment)	US-PGPUB; USPAT	AND	ON	2017/11/16 12:42
L18	55	((movement or moving)(path or direction)(camera)(authenticat$4 or identity)(register$4 or	US-PGPUB; USPAT;	AND	ON	2017/11/16 12:42

		enroll$4 or enrollment)).clm.	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
L20	23467	(authenticat$4 or identity)(camera)(threshold or meet$4)(movement or moving or path or direction)same(camera or mobile or smartphone)same(user or hand or particular or expected)same(path or parameter or direction or area or display)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/11/16 12:43
L21	21384	L20 (image or picture)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/11/16 12:44
L22	9622	L20 (image or picture).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/11/16 12:44
L23	3255	L20 (image or picture or biometric).clm. (authenticat$4 or identity or biometric or face or facial).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/11/16 12:45
L24	383	L17 or L18	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/11/16 12:45
L25	2226	L23 (path or parameter)(threshold or expected)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/11/16 12:46
L26	1467	L23 (path or parameter)(threshold)(meet$4 or expected)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/11/16 12:46
L27	132	L24 L26	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/11/16 12:46

L28	1718	L24 OR L26	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/11/16 12:46
L29	388	L28(movement or moving or path or direction)near5(camera or mobile or smart$phone)(authenticat$4 or identity) (register$4 or enroll$4 or enrollment or authenticat$4).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/11/16 12:48
L30	1084	L28(predetermined or expected or area or sequential$4 or screen or size or place or region)same(display$4 or camera or image or picture or face or head or user)same(mobile or camera or smart$phone)(authenticat$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/11/16 12:51
L31	73	("5031228" "5699449" "5784056" "5835616" "6212030" "6461807" "6961361" "7211138" "7460916" "7710693" "7960470" "8210247" "8460024" "8709801" "8959578" "9209355" "9459132" "9708909" "9958687" "10208464" "10458241" "10957795" "11207572" "11457349" "5031228" "5699449").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/11/16 12:57
L32	74	"20040070678" "20040081338" "20040125991" "20040143598" "20040190758" "20040109584" "20040201709" "200470264780" "20050094849" "20050117802" "20050141766" "20050180627" "20050190273" "20050220347" "20050251015" "20050265603" "20160261675" "20160259528" "20150153571" "20150131872"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/11/16 13:01
L33	68	("9076028" "9076008" "9137246" "9152849" "9202105" "9424491" "9430695" "8649604" "8743051" "8750574").pn. "20130267204" "20130342672" "20140012756" "20140059673" "20140118257" "20140165187" "20140169643" "20140198959"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/11/16 13:05
L34	37	"9607138".pn. "8856541".pn. "20140198959" "20140165187" "20140059673" "20140123275" "20140337948" "20140169643" "20140169643" "20150378433"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/11/16 13:07
L35	236	L31 OR L32 OR L33 OR L34	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/11/16 13:08
L36	1113	L29 OR L30	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2017/11/16 13:08

			DERWENT; IBM_TDB			
L37	1342	L35 L36	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/11/16 13:09
L38	7	L35 L36	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/11/16 13:09
L39	1156	L36 OR L27	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/11/16 13:11
L40	186	L39 (G06F21/32 OR G06F21/34 OR G06K9/00255 OR G06K9/00912 OR G06K9/00926 OR G06K9/22 OR G06Q20/3276 OR G06Q20/40145).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/11/16 13:13
L41	367	L27 OR L35	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/11/16 13:13
L42	22	L40 L41	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/11/16 13:13

11/16/2017 1:16:10 PM
C:\Users\sabedin\Documents\EAST\Workspaces\14570611.wsp

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	186	("10208464" | "10458241" | "10957795" | "11207572" | "11457349" | "20030236832" | "20040070678" | "20040081338" | "20040109584" | "20040125991" | "20040143598" | "20040190758" | "20040201709" | "200470264780" | "20050031173" | "20050065855" | "20050094849" | "20050100195" | "20050117802" | "20050141766" | "20050180627" | "20050190273" | "20050220347" | "20050251015" | "20050265603" | "20060050933" | "20060110014" | "20060133672" | "20060156029" | "20060173560" | "20060218225" | "20060222215" | "20060239515" | "20060251292" | "20060251338" | "20060251339" | "20060253491" | "20060274978" | "20070074114" | "20070081744" | "20070098303" | "20070177805" | "20070206834" | "20070211925" | "20080046458" | "20080077595" | "20080080743" | "20080080745" | "20080091723" | "20080130960" | "20080212849" | "20080317379" | "20090185784" | "20090226052" | "20090232367" | "20090252383" | "20090324018" | "20090324022" | "20090324137" | "20100050134" | "20100054600" | "20100054601" | "20100061631" | "20100067750" | "20100158327" | "20100232656" | "20100245614" | "20100272363" | "20100287053" | "20100317420" | "20100318366" | "20110063108" | "20110169853" | "20110202531" | "20110225481" | "20110282906" | "20120323704" | "20130007032" | "20130057693" | "20130066526" | "20130077835" | "20130179298" | "20130226740" | "20130246158" | "20130267204" | "20130342672" | "20140012756" | "20140059673" | "20140118257" | "20140165187" | "20140169643" | "20140198959" | "20140337948" | "20150052462" | "20150055821" | "20150077323" | "20150131872" | "20150153571" | "20150310260" | "20150378433" | "20160063235" | "20160209939" | "20160259528" | "20160261675" | "20160342826" | "20170220843" | "2140098174" |	US-PGPUB; USPAT	OR	OFF	2017/12/01 20:52

		"5031228" | "5699449" | "5784056" | "5835616" | "6212030" | "6461807" | "6678664" | "6687390" | "6697502" | "6728401" | "6775397" | "6840149" | "6961361" | "7003135" | "7211138" | "7218774" | "7231657" | "7289648" | "7308581" | "7333963" | "7415152" | "7460916" | "7519200" | "7636450" | "7646909" | "7660444" | "7710693" | "7788247" | "7804982" | "7809722" | "7945653" | "7960470" | "8121408" | "8165352" | "8210247" | "8244211" | "8316237" | "8326000" | "8392268" | "8396246" | "8416312" | "8460024" | "8649604" | "8709801" | "8743051" | "8750574" | "8788977" | "8856541" | "8867849" | "8922480" | "8959578" | "9037354" | "9076008" | "9076028" | "9137246" | "9152849" | "9202105" | "9209355" | "9424491" | "9430695" | "9459132" | "9600649" | "9607138" | "9708909" | "9740848" | "9958687" | "D650793" | "D667423" | "D726221" | "D737325" | "D753132" | "D756401" | "D762655" | "D762673" | "D762715" | "D763271" | "D765674" | "D769933" | "D776680" | "D778923" | "D778940" | "D780781" | "D783633" | "D783652" | "D784363" | "D787527" | "D788122").PN.				
L2	38	("0000011" | "0002014" | "20030095053" | "20060224523" | "20120000006" | "20130000124" | "20140022179" | "20140173443" | "20140337791" | "20140351761" | "20150074615" | "20150148106" | "20150205399" | "20150205454" | "20150212684" | "20150227286" | "20160026425" | "D596192" | "D601582" | "D625325" | "D640277" | "D692018" | "D702714" | "D715317" | "D717339" | "D725151" | "D725668" | "D728623" | "D730389" | "D730941" | "D731552" | "D733755" | "D736812" | "D738921" | "D740833" | "D742417" | "D745567" | "D747354").PN.	US-PGPUB; USPAT	OR	OFF	2017/12/01 20:53
L3	2	("20120140993" | "20140123275").PN.	US-PGPUB; USPAT	OR	OFF	2017/12/01 20:53
L4	6	("0000411" | "20100310133" | "5956122" | "7428320" | "8280120" | "8411909").PN.	US-PGPUB; USPAT	OR	OFF	2017/12/01 20:53
L6	232	L1 OR L2 or L3 OR L4	US-PGPUB; USPAT	OR	OFF	2017/12/01 20:54
L7	16453	(G06F21/32 OR G06F21/34 OR G06K9/00255 OR G06K9/00912 OR G06K9/00926 OR G06K9/22 OR G06Q20/3276 OR G06Q20/40145).cpc.	US-PGPUB; USPAT	AND	OFF	2017/12/01 20:54
L9	4730	L7(predetermined or expected or area or sequential$4 or screen or size or place or region)same(display$4 or camera or image or picture or face or head or user)same(mobile or camera or smart$phone)(authenticat$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2017/12/01 20:55

L10	520	L7((path or parameter)(threshold) (meet$4 or expected))(biometric) (authenticat$4)(image or picture or photo).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 20:56
L11	578	L9(authenticat$4 or identity)(camera) (threshold or meet$4)(movement or moving or path or direction)same(camera or mobile or smartphone)same(user or hand or particular or expected)same(path or parameter or direction or area or display)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 20:56
L12	46	L7 (movement or moving or path or direction)near5(camera or mobile or smartphone)same(user or hand or particular or expected or head or face or determin$4)same(path or parameter or direction or area or display or sequential$4 or predetermined).clm.(authenticat$4 or identity or enroll$5 or register$4).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 20:57
L13	330	L7 (movement or moving)(path or direction)(movement or moving or path or direction)near5(camera or mobile or smartphone)same(user or hand or particular or expected or head or face or determin$4)same(path or parameter or direction or area or display or sequential$4 or predetermined)(authenticat$4 or identity)(enroll$5 or register$4 or registration)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 20:58
L14	1154	L10 or L11 or L12 or L13	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 20:58
L15	16	L6 L14	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 20:58
L16	1370	L6 OR L14	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 20:58
L17	37	"9607138".pn. "8856541".pn. "20140198959" "20140165187" "20140059673" "20140123275" "20140337948" "20140169643" "20150378433"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/12/01 21:01
L18	48	L15 or L17	US-PGPUB;	OR	ON	2017/12/01

			USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			21:01
L19	42	L18 @ad<"20140828"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 21:02
L20	812	L16 (movement or displacement or moving or displaced or predetermined or sensor)same(direction or parameter or threshold or path or expected)same(image or picture or camera or smartphone or expected)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 21:05
L21	746	L7 L20	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 21:05
L22	255	(L11)(L10 or L13)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 21:06
L23	192	L21 L22	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 21:06
L24	172	L23 (face)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 21:06
L25	72	L23 (face)same(display or screen)same(area or region)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 21:06
L26	72	L23 (face)same(display or screen)same(area or region) (authenticat$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	AND	ON	2017/12/01 21:07

			IBM_TDB			
L27	26	L26 @ad<"20140828"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 21:07
L29	64	L19 or L27	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 21:07
L30	27	L29(face)same(display or screen)same(area or region) (authenticat$4)(path or direction) (movement or moving or displacing or displacement)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 21:09
L31	17	L29(face)same(display or screen)same(area or region) (authenticat$4)(path or direction) (movement or moving or displacing or displacement)(mobile or smartphone or camera).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 21:09
L33	48	L15 or L17	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 21:09
L34	4	L31 L33	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 21:10
L35	61	L31 OR L33	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 21:10
L36	15	L35(face or facial or sequential$4 or sequence or hold$4)same(display or screen or area or region)(authenticat$4) (path or direction or movement or moving or displacing or displacement).clm.(mobile or smartphone or camera or parameter).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 21:11
L37	14	L35(face or facial or sequential$4 or sequence or hold$4)same(display or screen or area or region)(authenticat$4) (path or direction or movement or moving	US-PGPUB; USPAT; USOCR; FPRS;	AND	ON	2017/12/01 21:11

		or displacing or displacement).clm.(mobile or smartphone or camera or parameter).clm.(threshold)	EPO; JPO; DERWENT; IBM_TDB			
L38	17	L34 OR L37	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 21:12
L39	10	L38 NOT L17	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 21:12
L40	9	L39 @ad<"20140828"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2017/12/01 21:13

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L41	1041	(face or facial or sequential$4 or sequence or hold$4)same(display or screen or area or region)(authenticat$4)(path or direction or movement or moving or displacing or displacement).clm.(mobile or smartphone or camera or parameter).clm.(threshold).clm.	US-PGPUB; USPAT	AND	ON	2017/12/01 21:17
L42	1848	(face)same(display or screen)same(area or region)(authenticat$4)(path or direction) (movement or moving or displacing or displacement)(mobile or smartphone or camera).clm.	US-PGPUB; USPAT	AND	ON	2017/12/01 21:17
L44	1028	(movement or moving or path or direction)near5(camera or mobile or smartphone)same(user or hand or particular or expected or head or face or determin$4)same(path or parameter or direction or area or display or sequential$4 or predetermined).clm.(authenticat$4 or identity or enroll$5 or register$4).clm.	US-PGPUB; USPAT	AND	ON	2017/12/01 21:17
L45	28327	(predetermined or expected or area or sequential$4 or screen or size or place or region)same(display$4 or camera or image or picture or face or head or user)same(mobile or camera or smart$phone) (authenticat$4).clm.	US-PGPUB; USPAT	AND	OFF	2017/12/01 21:17
L46	31536	L41 OR L42 OR L44 OR L45	US-PGPUB; USPAT	AND	ON	2017/12/01 21:20
L47	186	("10208464" | "10458241" | "10957795" | "11207572" | "11457349" | "20030236832" | "20040070678" | "20040081338" |	US-PGPUB; USPAT	OR	OFF	2017/12/01 21:21

		"20040109584" | "20040125991" |					
		"20040143598" | "20040190758" |					
		"20040201709" | "200470264780" |					
		"20050031173" | "20050065855" |					
		"20050094849" | "20050100195" |					
		"20050117802" | "20050141766" |					
		"20050180627" | "20050190273" |					
		"20050220347" | "20050251015" |					
		"20050265603" | "20060050933" |					
		"20060110014" | "20060133672" |					
		"20060156029" | "20060173560" |					
		"20060218225" | "20060222215" |					
		"20060239515" | "20060251292" |					
		"20060251338" | "20060251339" |					
		"20060253491" | "20060274978" |					
		"20070074114" | "20070081744" |					
		"20070098303" | "20070177805" |					
		"20070206834" | "20070211925" |					
		"20080046458" | "20080077595" |					
		"20080080743" | "20080080745" |					
		"20080091723" | "20080130960" |					
		"20080212849" | "20080317379" |					
		"20090185784" | "20090226052" |					
		"20090232367" | "20090252383" |					
		"20090324018" | "20090324022" |					
		"20090324137" | "20100050134" |					
		"20100054600" | "20100054601" |					
		"20100061631" | "20100067750" |					
		"20100158327" | "20100232656" |					
		"20100245614" | "20100272363" |					
		"20100287053" | "20100317420" |					
		"20100318366" | "20110063108" |					
		"20110169853" | "20110202531" |					
		"20110225481" | "20110282906" |					
		"20120323704" | "20130007032" |					
		"20130057693" | "20130066526" |					
		"20130077835" | "20130179298" |					
		"20130226740" | "20130246158" |					
		"20130267204" | "20130342672" |					
		"20140012756" | "20140059673" |					
		"20140118257" | "20140165187" |					
		"20140169643" | "20140198959" |					
		"20140337948" | "20150052462" |					
		"20150055821" | "20150077323" |					
		"20150131872" | "20150153571" |					
		"20150310260" | "20150378433" |					
		"20160063235" | "20160209939" |					
		"20160259528" | "20160261675" |					
		"20160342826" | "20170220843" |					
		"2140098174" | "5031228" | "5699449" |					
		"5784056" | "5835616" | "6212030" |					
		"6461807" | "6678664" | "6687390" |					
		"6697502" | "6728401" | "6775397" |					
		"6840149" | "6961361" | "7003135" |					
		"7211138" | "7218774" | "7231657" |					
		"7289648" | "7308581" | "7333963" |					
		"7415152" | "7460916" | "7519200" |					
		"7636450" | "7646909" | "7660444" |					
		"7710693" | "7788247" | "7804982" |					
		"7809722" | "7945653" | "7960470" |					
		"8121408" | "8165352" | "8210247" |					
		"8244211" | "8316237" | "8326000" |					
		"8392268" | "8396246" | "8416312" |					
		"8460024" | "8649604" | "8709801" |					

		"8743051" | "8750574" | "8788977" | "8856541" | "8867849" | "8922480" | "8959578" | "9037354" | "9076008" | "9076028" | "9137246" | "9152849" | "9202105" | "9209355" | "9424491" | "9430695" | "9459132" | "9600649" | "9607138" | "9708909" | "9740848" | "9958687" | "D650793" | "D667423" | "D726221" | "D737325" | "D753132" | "D756401" | "D762655" | "D762673" | "D762715" | "D763271" | "D765674" | "D769933" | "D776680" | "D778923" | "D778940" | "D780781" | "D783633" | "D783652" | "D784363" | "D787527" | "D788122").PN.				
L48	2	("20120140993" | "20140123275").PN.	US-PGPUB; USPAT	OR	OFF	2017/12/01 21:21
L49	6	("0000411" | "20100310133" | "5956122" | "7428320" | "8280120" | "8411909").PN.	US-PGPUB; USPAT	OR	OFF	2017/12/01 21:21
L50	38	("0000011" | "0002014" | "20030095053" | "20060224523" | "20120000006" | "20130000124" | "20140022179" | "20140173443" | "20140337791" | "20140351761" | "20150074615" | "20150148106" | "20150205399" | "20150205454" | "20150212684" | "20150227286" | "20160026425" | "D596192" | "D601582" | "D625325" | "D640277" | "D692018" | "D702714" | "D715317" | "D717339" | "D725151" | "D725668" | "D728623" | "D730389" | "D730941" | "D731552" | "D733755" | "D736812" | "D738921" | "D740833" | "D742417" | "D745567" | "D747354").PN.	US-PGPUB; USPAT	OR	OFF	2017/12/01 21:21
L51	14	"9607138".pn. "8856541".pn. "20140198959" "20140165187" "20140059673" "20140123275" "20140337948" "20140169643" "20150378433"	US-PGPUB; USPAT	OR	ON	2017/12/01 21:21
L52	2	"20140197922" "20130342672"	US-PGPUB; USPAT	OR	ON	2017/12/01 21:21
L53	238	L47 or L48 or L49 or L50 or L51 or L52	US-PGPUB; USPAT	OR	ON	2017/12/01 21:22
L54	35	L46 L53	US-PGPUB; USPAT	AND	ON	2017/12/01 21:22
L55	31	L54 @ad<"20140828"	US-PGPUB; USPAT	AND	ON	2017/12/01 21:23
L56	27	L55 (biometric or image or picture) (authenticat$4 or identity).clm.	US-PGPUB; USPAT	AND	ON	2017/12/01 21:23
L57	2	L56(movement or moving or path or direction)near5(camera or mobile or smartphone)same(user or hand or particular or expected or head or face or determin$4)same(path or parameter or	US-PGPUB; USPAT	AND	ON	2017/12/01 21:24

		direction or area or display or sequential$4 or predetermined).clm.(authenticat$4 or identity or enroll$5 or register$4).clm.				
L58	9	L56(predetermined or expected or area or sequential$4 or screen or size or place or region)same(display$4 or camera or image or picture or face or head or user)same(mobile or camera or smart$phone).clm. (authenticat$4).clm.	US-PGPUB; USPAT	AND	OFF	2017/12/01 21:24
L59	10	L57 or L58	US-PGPUB; USPAT	AND	OFF	2017/12/01 21:24
L60	7	L59(predetermined or expected or threshold or met or match$4)same(area or sequential$4 or screen or region or display$4 or parameter or input)same(display$4 or camera or image or picture or face or head or facial).clm. (mobile or camera or smart$phone).clm. (authenticat$4 or identity).clm.	US-PGPUB; USPAT	AND	OFF	2017/12/01 21:28
L61	1	L60 NOT L51	US-PGPUB; USPAT	AND	OFF	2017/12/01 21:28
L62	4	L60(mobile or camera or smart$phone)near7(moving or holding or movement or displacement or displaced or moved).clm.	US-PGPUB; USPAT	AND	OFF	2017/12/01 21:30
L63	2	L60(mobile or camera or smart$phone)near7(moving or holding or movement or displacement or displaced or moved)same(direction or predetermined).clm.	US-PGPUB; USPAT	AND	OFF	2017/12/01 21:31
L64	0	L60(Path or parameter).clm.	US-PGPUB; USPAT	AND	OFF	2017/12/01 21:31
L65	3	L61 OR L63	US-PGPUB; USPAT	AND	OFF	2017/12/01 21:31
L66	0	L59(area or region or sequential$4)near5(display or screen)same(face or head)	US-PGPUB; USPAT	AND	OFF	2017/12/01 21:33
L67	0	L59(Path or parameter).clm.	US-PGPUB; USPAT	AND	OFF	2017/12/01 21:33
L68	0	L65(area or region or sequential$4 or path)near5(display or screen or parameter)same(face or movement).clm.	US-PGPUB; USPAT	AND	OFF	2017/12/01 21:34
L69	0	L65(area or region or sequential$4 or path)near5(display or screen or parameter)same(face or movement) (threshold).clm.	US-PGPUB; USPAT	AND	OFF	2017/12/01 21:34

12/1/2017 9:35:14 PM
C:\Users\sabedin\Documents\EAST\Workspaces\14570611.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14839505	TUSSY, KEVIN ALAN
	Examiner	Art Unit
	SHANTO M ABEDIN	2436

CPC- SEARCHED		
Symbol	Date	Examiner
CPC search: (G06F21/34 OR G06F21/32 OR G06F21/6218OR H04L63/0861).cpc.	06/28/2017	SA
CPC Search: (G06F21/32 OR G06F21/34 OR G06K9/00255OR G06K9/00912 OR G06K9/00926 OR G06K9/22OR G06Q20/3276 OR G06Q20/40145).cpc.	12/01/2017	SA

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	6-7	06/28/2017	SA
713	168, 182	06/28/2017	SA
455	410, 411	06/28/2017	SA

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor Assignee/ Double Patenting search	06/28/2017	SA
CPC and USPC classification search (with limited texts)	06/28/2017	SA
EAST databases text search (see search history)	06/28/2017	SA
EAST databases text search (see search history)	06/29/2017	SA
NPL: Google Scholar, IEEE Xplore databases search (see search history)	07/09/2017	SA
EAST databases including PGPUB, USPAT, EPO, JPO, IBM_TDB text search (see search history)	12/01/2017	SA
NPL: Google Scholar, IEEE Xplore, ACM databases search (see search history)	12/06/2017	SA

INTERFERENCE SEARCH			
US Class/ CPC Symbol	**US Subclass / CPC Group**	**Date**	**Examiner**
Claim Interference Search	See EAST Search History	06/29/2017	SA
Claim Interference Search	See EAST Search History	12/01/2017	SA

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor	:	Kevin Alan Tussy	)
			) Group Art Unit: 2436
Appl. No.	:	14/839,505	)
			) I hereby certify that this correspondence and all marked attachments are being deposited with the United States Patent Office via EFSWeb filing, on:
Filed	:	August 28, 2015	)
			) October 5, 2017 (Date)
For	:	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS	) /Chad W. Miller/ Chad W. Miller Reg. No. 44,943
			)
Examiner	:	Shanto Abedin	)

RESPONSE TO OFFICE ACTION

Mail Stop Amendment
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This is in response to the Office Action mailed July 17, 2017 with respect to the above-referenced application. Please amend the application as follows:

IN THE CLAIMS:

1. (currently amended) A method for enrolling and authenticating a user in an authentication system via the ~~a~~ user's ~~a~~ mobile ~~computing~~ device comprising a camera and at least one movement detecting sensor, the method comprising:

capturing enrollment biometric information from at least one first image of the user, the first image recorded by the camera of the mobile device;

storing the enrollment biometric information on a memory;

during an authentication session:

capturing authentication biometric information from at least one second image of the user, the second image recorded by the camera of the mobile device;

recording~~, during imaging of the at least one second image,~~ path parameter data from the at least one movement detecting sensor in the mobile device, the path parameter data generated by movement of the mobile device by the user and representing an authentication movement of the mobile device;

comparing the authentication biometric information to the stored enrollment biometric information to determine whether the authentication biometric information meets a predetermine similarity threshold as compared to the enrollment biometric information;

comparing the authentication movement of the mobile device to an expected movement of the mobile device to determine whether the authentication movement meets a predetermine similarity threshold as compared to the expected movement of the mobile device by the user; and

when the authentication biometric information sufficiently corresponds with the enrollment biometric information, and when the authentication movement meets a predetermine similarity threshold as compared to ~~with~~ the expected movement, authenticating the user.

2. (original) The method according to claim 1, further comprising capturing, during imaging of the at least one first image, enrollment path parameters via the at least one movement detecting sensor, the enrollment path parameters indicating an enrollment movement of the mobile device, and defining the expected movement as the enrollment movement.

3. (original) The method according to claim 1, wherein the at least one first image and the at least one second image of the user include an image of the user's face, and the enrollment biometric information and the authentication biometric information comprise facial recognition information.

4. (original) The method according to claim 1, further comprising:

capturing enrollment device information during imaging of the at least one first image;

storing the enrollment device information on the memory;

capturing authentication device information during imaging of the at least on second image; and

comparing the authentication device information with the enrollment device information to determine whether the authentication device information sufficiently corresponds to the enrollment device information.

5. (original) The method according to claim 4, wherein the device information comprises at least one of the following: a device manufacturer, model number, serial number, and mobile network information.

6. (original) The method according to claim 1, wherein at least one movement detecting sensor comprises at least one of the following: an accelerometer, a magnetometer, and a gyroscope.

7. (currently amended) A facial authentication system utilizing a user's mobile device, the mobile device comprising a camera and at least one movement detecting sensor, the authentication system comprising:

an authentication server comprising a processor, a memory, and at least one transceiver configured to transmit data from the authentication server and received data;

one or more memories configured to store one or more databases, the one or more databases configured to store authentication information profiles; and

machine readable instructions that are stored on the memory of the authentication server which when executed by the processor, cause the authentication server to:

receive enrollment biometrics from the mobile device, the enrollment biometrics comprising facial recognition data processed from at least one first image of the user's face obtained via the camera of the mobile device;

store the enrollment biometrics in the one or more databases and associate the enrollment biometric data with the user authentication information profile;

receive authentication biometrics from the mobile device during an authentication attempt by the user, the authentication biometrics comprising facial recognition data processed from at least one second image of the user's face, the image obtained from the camera of the mobile device;

receive authentication movement information from the mobile device, the authentication movement information comprising data regarding movement of the mobile

device ~~during imaging of the at least one second image~~ as detected by the at least one movement detecting sensor in the mobile device;

compare the authentication biometrics and the authentication movement information with the enrollment biometrics and expected movement information stored in the database with the user authentication information profile such that the expected movement is based on an anticipated path of the mobile device to place the user's face sequentially in a first display area and a second display area; and

authenticate or not authenticate the user based on a comparison match rate of the authentication biometrics and the authentication movement with the enrollment biometrics and the expected movement.

8. (currently amended) The facial authentication system of claim 7, wherein

the mobile device displays a first prompt on a display screen to instruct the user to position the user's face ~~a face of the user~~ within the ~~a~~ first display area of the display screen,

the mobile device display a second prompt on the display screen to instruct the user to position the user's face ~~of the user~~ within the ~~a~~ second display area of the display screen, the second display area being a different size than the first display area. ~~, and~~

~~the expected movement is based on an anticipated path of the mobile device to place the face sequentially in the first display area and the second display area.~~

9. (original) The facial authentication system of claim 7, wherein the authentication server detects the presence or absence of banding in the at least one second image.

10. (original) The facial authentication system of claim 7, wherein the authentication server detect the present or absence of a screen edge in the at least one second image.

11. (original) The facial authentication system of claim 7, wherein

the authentication server or mobile device estimates at least one of a gender, age, and ethnicity of a face imaged in the at least one first image,

the authentication server estimates at least one of a gender, age, and ethnicity of the face imaged in the at least one second image, and

the authentication server authenticates or does not authenticate the user based on a comparison match rate of at least one of a gender, age, and ethnicity detected in the at least one first image and the at least one second image in relation to a comparison match rate threshold.

12. (original) The facial authentication system of claim 7, wherein the comparison match rate threshold required for authentication is variable.

13. (original) The facial authentication system of claim 12, wherein the comparison match rate threshold increases based on a number of successful authentications.

14. (original) The facial authentication system of claim 12, wherein the comparison match rate threshold increases over time.

15. (canceled)

16. (canceled)

17. (canceled)

18. (canceled)

19. (canceled)

20. (canceled)

21. (canceled)

22. (new) A facial authentication system utilizing a user's mobile device, the mobile device comprising a camera and at least one movement detecting sensor, the authentication system comprising:

a processor located in the mobile device configured to execute machine readable instructions;

one or more memories in the mobile device storing authentication information and

non-transitory machine readable instructions, the machine readable instructions when executed by the processor cause the mobile device to:

receive enrollment biometrics, the enrollment biometrics comprising facial recognition data processed from at least one first image of the user's face obtained via the camera of the mobile device;

store the enrollment biometrics in the memory of the mobile device and associate the enrollment biometric data with the user;

receive authentication biometrics from the mobile device during an authentication attempt by the user, the authentication biometrics comprising facial recognition data processed from at least one second image of the user's face, the image obtained from the camera of the mobile device during the authentication attempt;

receive authentication movement information from the mobile device, the authentication movement information comprising data generated during movement of the mobile device by the user during the authentication attempt as detected by the at least one movement detecting sensor in the mobile device;

compare the authentication biometrics and the authentication movement information with the enrollment biometrics and expected movement information stored in the mobile device, such that the expected movement information is based on an anticipated path of the mobile device to place the user's face sequentially in a first display area and a second display area; and

authenticate or not authenticate the user during the authentication attempt based on a comparison match rate of the authentication biometrics and the authentication movement information with the enrollment biometrics and the expected movement information.

23. (new) The system of claim 22 wherein the first display area is a different size than the second display area.

24. (new) The system of claim 22 wherein the compare also detects the presence or absence of banding in the at least one second image.

25. (new) The system of claim 22 wherein the compare also detects the present or absence of a screen edge in the at least one second image.

26. (new) The system of claim 22 wherein the anticipated path of the mobile device is a path of the mobile device between a first mobile device position and a second mobile device position, such that the first position is a different distance from the user than the second distance.

27. (new) The system of claim 22 wherein:

non-transitory machine readable instructions, stored on the one or more memory of the mobile device, which when executed by the processor also estimates at least one of a gender, age, and ethnicity of a face imaged in the at least one first image, and estimates at least one of a gender, age, and ethnicity of the face imaged in the at least one second image, and

authenticates or does not authenticate the user based on a comparison match rate of at least one of a gender, age, and ethnicity detected in the at least one first image and the at least one second image in relation to a comparison match rate threshold.

REMARKS

This Response is in reply to the Office Action mailed July 17, 2017. In the Office Action, the Examiner objected to claim 8 and further rejected claims 1-7 and 9-21. Claims 1-3, 7, 11-18 and 20 are rejected under 35 U.S.C. § 103(b) as being unpatentable over U.S. Pub. 2014/0123275 to Azar, et al., in view of U.S. Pub. 2014/0165187 to Daesung, et al. Claims 4-6, 9-10 and 21 are rejected under 35 U.S.C. § 103(b) as being unpatentable over the Azar, et al. reference, in view of the Daesung, et al., reference further view of U.S. Pat. 9,607,138 to Baldwin, et al. Claim 19 is rejected under 35 U.S.C. § 103(b) as being unpatentable over the Azar, et al. reference, in view of the Daesung, et al. reference, further view of U.S. Pub. 2014/0169643 to Todoroki.

Claims 1-6

The Applicant amends claim 1 to make clear that the path parameter data is generated by movement of the mobile device by the user. This is in contrast to the Daesung reference, cited by the Examiner, which teaches that the face movement pattern is in fact facial expressions, such as "number of blinks of eyes, a rotation direction of a head and a movement direction" of a user's face (see paragraphs [0038] and [0039]). In contrast, the method of claim 1 is directed to a method in which the mobile device moves, which in turn causes movement sensors in the mobile device to generate movement data. This movement data which is generated during an authentication attempt is compared to expected and known movement data for a match or sufficient similarity as part of the authentication attempt. This feature, in combination with the comparison of the biometric information from a first image (captured during enrollment) and the second image (captured during authentication) provides benefits over the prior art. The prior art does not teach an authentication system having these features. For this reason, claim 1 is asserted to be allowable.

The Applicant submits that claims 2-6 are also allowable based on the dependence of these claims from allowable claim 1.

Claims 7-14

In the Office Action, the Examiner objected to claim 8 and indicated that claim 7 would be allowable if the limitations from claim 8 were included in claim 7. During the telephonic conference, the Examiner indicated that the last element of claim 8 is the subject matter that differentiated claim 8 from the prior art. In response, the Applicant amends claim 7 with the last element from claim 8. As a result, and for the reasons set forth above for claim 1, the Applicant asserts that claim 7 as amended is allowable. Claim 8 is amended as shown. Review and consideration is respectfully requested. The Applicant asserts that claims 8-14 are also allowable based on the dependence of these claims from allowable claim 7.

Claims 15-21

The Applicant cancels claims 15-21 but provides notice that they may pursue this subject matter in a continuation application based on the Examiner's suggestion that these claims may be directed to a different invention. These claims are not being canceled based on the prior art or any rejection, but instead due to the nature of claimed subject matter based on the Examiner's helpful comments.

New Claims 22-27

The Applicant adds new claims 22-27. Claim 22 is directed to generally similar subject matter as claim 7. Claim 22 is modified to have the method performed on the mobile device instead of an authentication server. The specification supports this embodiment at least at paragraphs [0045] - [0048], and [0055] - [0056]. The method that is the focus of the claims is

generally similar between claim 7 and new claim 22. Having the novel method execute on the mobile device, instead of an authentication server, does not necessitate a restriction requirement for claim 22 due to the method of operation being similar albeit with a different execution platform. The Applicant asserts that claims 23-37 are also allowable based on the dependence of these claims from allowable claim 22.

Summary

Applicant asserts that claims 1-14 and 22-27 are in a condition for allowance and respectfully requests a notice as to the same. If any matters remain outstanding, the Examiner is invited to contact the undersigned by telephone.

Respectfully submitted,

Dated: October 5, 2017

By: /Chad W. Miller/

Chad W. Miller
Attorney of Record
Registration No. 44,943
Weide & Miller, Ltd.
7251 West Lake Mead Blvd., Suite 530
Las Vegas, NV 89128
(702) 382-4804 (Pacific Time)
cmiller@weidemiller.com

Electronic Acknowledgement Receipt	
EFS ID:	30581851
Application Number:	14839505
International Application Number:	
Confirmation Number:	6236
Title of Invention:	Facial Recognition Authentication System Including Path Parameters
First Named Inventor/Applicant Name:	Kevin Alan Tussy
Customer Number:	32856
Filer:	Chad W. Miller
Filer Authorized By:	
Attorney Docket Number:	FACIAL.0012P
Receipt Date:	05-OCT-2017
Filing Date:	28-AUG-2015
Time Stamp:	19:37:57
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		CWMW12241V2OAR.pdf	58970 b6d4883556c76c0b044333a383a8ebd8233b9383	yes	12

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	9
	Applicant Arguments/Remarks Made in an Amendment	10	12
Warnings:			
Information:			
	Total Files Size (in bytes):	58970	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/839,505	Filing Date 08/28/2015	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)		
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)		
	10/05/2017	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
AMENDMENT	Total (37 CFR 1.16(i))	* 20	Minus	** 21	= 0	X $40 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $210 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)		
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
AMENDMENT	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
NICOLLE L. SCRIVNER

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		5,031,228	07/91	Lu			
		5,699,449	12/97	Javidi			
		5,784,056	07/98	Nielsen			
		5,835,616	11/98	Lobo, et al.			
		6,212,030	07/91	Lu			
		6,461,807	12/97	Javidi			
		6,961,361	11/98	Lobo, et al.			
		7,211,138	07/91	Lu			
		7,460,916	12/97	Javidi			
		7,710,693	07/98	Nielsen			
		7,960,470	11/98	Lobo, et al.			
		8,210,247	07/91	Lu			
		8,460,024	12/97	Javidi			
		8,709,801	07/98	Nielsen			
		8,959,578	11/98	Lobo, et al.			
		9,209,355	07/91	Lu			
		9,459,132	12/97	Javidi			
		9,708,909	07/98	Nielsen			
		9,958,687	11/98	Lobo, et al.			
		10,208,464	07/91	Lu			
		10,458,241	12/97	Javidi			
		10,957,795	11/98	Lobo, et al.			
		11,207,572	07/91	Lu			
		11,457,349	12/97	Javidi			
		5,031,228	07/91	Lu			
		5,699,449	12/97	Javidi			

EXAMINER	DATE CONSIDERED

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2003/0236832	12/03	McIntyre, et al.			
		6,678,664	01/04	Ganesan			
		6,687,390	02/04	Avni			
		6,697,502	02/04	Luo			
		6,728,401	04/04	Hardeberg			
		2004/0070678	04/04	Toyama, et al.			
		2004/0081338	04/04	Takenaka			
		2004/0125991	07/04	Yokoi			
		2004/0143598	07/04	Drucker, et al.			
		6,775,397	08/04	Hamalainen			
		2004/0190758	09/04	Doi, et al.			
		2004/0109584	10/04	Lestideau			
		2004/0201709	10/04	McIntyre, et al.			
		6,840,149	10/04	Squilla, et al.			
		20047/0264780	12/04	Zhang, et al.			
		2005/0031173	02/05	Hwang			
		2005/0065855	03/05	Geller			
		2005/0094849	05/05	Sung, et al.			
		2005/0100195	05/05	Li			
		2005/0117802	06/05	Yonaha, et al.			
		2005/0141766	06/05	Nagahashi, et al.			
		2005/0180627	08/05	Yang, et al.			
		2005/0190273	09/05	Toyama, et al.			
		2005/0220347	10/05	Enomoto			
		2005/0251015	11/05	Takikawa, et al.			
		2005/0265603	12/05	Porter, et al.			

EXAMINER	DATE CONSIDERED

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		7,003,135	02/06	Hsieh, et al.			
		2006/0050933	03/06	Adam, et al.			
		2006/0110014	05/06	Philomin			
		2006/0133672	06/06	Li			
		2006/0156029	07/06	Algazi			
		2006/0173560	08/06	Widrow			
		2006/0218225	09/06	Hee Voon, et al.			
		2006/0222215	10/06	Jung, et al.			
		2006/0239515	10/06	Zhang, et al.			
		2006/0251292	11/06	Gokturk, et al.			
		2006/0251338	11/06	Gokturk, et al.			
		2006/0251339	11/06	Gokturk, et al.			
		2006/0253491	11/06	Gokturk, et al.			
		2006/0274978	12/06	Fukuda, et al.			
		2007/0074114	03/07	Adjali			
		2007/0081744	04/07	Gokturk, et al.			
		2007/0098303	05/07	Gallagher, et al.			
		7,218,774	05/07	Liu			
		7,231,657	06/07	Honarvar			
		2007/177805	08/07	Gallagher			
		2007/0206834	09/07	Shinkai, et al.			
		2007/0211925	09/07	Aoki, et al.			
		7,289,648	10/07	Liu			
		7,308,581	12/07	Geosimonian			
		7,333,963	02/08	Widrow, et al.			
		2008/0046458	02/08	Tseng, et al.			

EXAMINER	DATE CONSIDERED

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2008/077595	03/08	Leebow			
		2008/0080743	04/08	Schneiderman, et al.			
		2008/0080745	04/08	Vanhoucke, et al.			
		2008/0091723	04/08	Zuckerberg, et al.			
		2008/0130960	06/08	Yagnik			
		7,415,152	08/08	Jiang, et al.			
		2008/0212849	09/08	Gao			
		2008/317379	12/08	Steinberg, et al.			
		7,519,200	04/09	Gokturk, et al.			
		2009/0185784	07/09	Hiroike, et al.			
		2009/0226052	09/09	Fedel			
		2009/232367	09/09	Shinzaki			
		2009/0252383	10/09	Adam, et al.			
		7,636,450	12/09	Bourdev			
		2009/0324018	12/09	Tell			
		2009/0324022	12/09	Sangberg, et al.			
		2009/0324137	12/09	Stallings, et al.			
		7,646,909	01/10	Jiang, et al.			
		7,660,444	02/10	Hamalainen			
		2010/0050134	02/10	Clarkson			
		20,100,067,750	03/10	Matsuo			
		2010/0054600	03/10	Anbalagan, et al.			
		2010/0054601	03/10	Anbalagan, et al.			
		2010/0061631	03/10	Omori			
		2010/0158327	06/10	Kangas, et al.			
		7,788,247	08/10	Wang, et al.			

EXAMINER	DATE CONSIDERED

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2010/0232656	09/10	Ryu			
		7,804,982	09/10	Howard, et al.			
		2010/245614	09/10	Matsunaga			
		7,809,722	10/10	Gokturk, et al.			
		2010/272363	10/10	Steinberg, et al.			
		2010/0287053	11/10	Ganong, et al.			
		2010/0318366	12/10	Sullivan			
		2010/0317420	12/10	Hoffberg			
		2,011,063,108	03/11	Aonuma, et al.			
		7,945,653	05/11	Zuckerberg, et al.			
		2011/0169853	07/11	Oiwa			
		2011/0202531	08/11	Zuckerberg, et al.			
		2011/0225481	09/11	Zuckerberg, et al.			
		2011/0282906	11/11	Wong			
		D650,793	12/11	Impas			
		8,121,408	02/12	Omori			
		8,165,352	04/12	Mohanty, et al.			
		8,244,211	08/12	Clark			
		D667,423	09/12	Nagamine			
		8,316,237	11/12	Felsher, et al.			
		2012/0323704	12/12	Steelberg			
		8,326,000	12/12	Jung, et al.			
		2013/0007032	01/13	Klappert			
		2013/0066526	03/13	Mondragon			
		8,392,268	03/13	Smith, et al.			
		2013/057693	03/13	Baranek			

EXAMINER	DATE CONSIDERED

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS							
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		8,396,246	03/13	Anbalagan, et al.			
		2013/077835	03/13	Kritt, et al.			
		8,416,312	04/13	Matsunaga			
		2013/0179298	07/13	Segman			
		2013/0226740	08/13	Biliosa			
		2013/0246158	09/13	Cannon			
		2013/0267204	10/13	Schultz			
		2013/0342672	12/13	Gray, et al.			
		2014/0012756	01/14	Beraja			
		2014/0059673	02/14	Azar			
		8,649,604	02/14	Steinberg, et al.			
		214/0098174	04/14	Summers			
		2014/0118257	05/14	Baldwin			
		2014/0165187	06/14	Daesung			
		2014/0169643	06/14	Todoroki			
		8,743,051	06/14	Moy, et al.			
		8,750,574	06/14	Ganong, et al.			
		2014/0198959	07/14	Derakhshani			
		8,788,977	07/14	Bezos			
		8,856,541	10/14	Chaudhury			
		8,867,849	10/14	Kirkham			
		2014/0337948	11/14	Hoyos			
		8,922,480	12/14	Freed, et al.			
		2015/0052462	02/15	Kulkarni			
		2015/0055821	02/15	Fotland			
		2015/0077323	03/15	Ramaswamy			

EXAMINER	DATE CONSIDERED
***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.	

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		D726,221	04/15	Gomez			
		9,037,354	05/15	Mondragon			
		2015/0131872	05/15	Ganong, et al.			
		2015/0153571	06/15	Ballard			
		9,076,028	07/15	Summers			
		9,076,008	07/15	Moy			
		D737,325	08/15	Kim			
		9,137,246	09/15	Parry, et al.			
		2015/0310260	10/15	Summers			
		9,152,849	10/15	Ganong, et al.			
		9,202,105	12/15	Wang, et al.			
		2015/0378433	12/15	Savastinuk			
		2016/0063235	03/16	Tussy			
		D753,132	04/16	Cuthbert			
		D756,401	05/16	Soldner			
		2016/0209939	07/16	Zambetti			
		9,424,491	08/16	Kirkham			
		9,430,695	08/16	Summers			
		D762,655	08/16	Kai			
		D762,673	08/16	Seo			
		D762,715	08/16	Williamson			
		D763,271	08/16	Everette			
		2016/0259528	09/16	Foss			
		2016/0261675	09/16	Block			
		D765,674	09/16	Kim			
		D769,933	10/16	Sabia			

EXAMINER	DATE CONSIDERED

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2016/0342826	11/16	Apostolos, et al.			
		D776,680	01/17	Bae			
		D778,923	02/17	Zhou			
		D778,940	02/17	Williamson			
		9,607,138	03/17	Baldwin			
		D780,781	03/17	Ding			
		9,600,649	03/17	Parry, et al.			
		D783,633	04/17	Oh			
		D783,652	04/17	Guan			
		D784,363	04/17	Fleming			
		D787,527	05/17	Wilberding			
		D788,122	05/17	Tada			
		9,740,848	08/17	Parry, et al.			
		2017/0220843	08/17	Apostolos, et al.			

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
							YES	NO
		EP 1388802	02/04	Europe			X	
		EP 1455297	09/04	Europe			X	
		WO 2006/130542	12/06	WIPO			X	
		WO 2008/107002	09/08	WIPO			X	
		WO 2015/070320	05/15	WIPO			X	

EXAMINER INITIAL	**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)	
		After Effects Tutorial - 17 - Introduction to Masking, by thenewboston, uploaded 12/07/2008, youtube.com [online], [retrieved 06/15/2017]. Available from <URL:https://www.youtube.com/watch?v=kWd51xDqzIc>

EXAMINER	DATE CONSIDERED

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

EXAMINER INITIAL		**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)
		Optical Illusions - Animated GIF & JPG, dated 10/28/2013, plus.google.com [online], [retrieved 06/19/2017]. Available from internet <URL:https://plus.google.com/+Whak-Off/posts/CX4YhzXSQy2>
		The Universal Face Login for 5 Billion Smartphones, zoomlogin.com [online], [retrieved 06/19/2017]. Available from internet <URL:https://zoomlogin.com/>
		Wong, Yongkang, et al. "Patch-based probabilistic image quality assessment for face selection and improved video-based face recognition." CVPR 2011 WORKSHOPS. IEEE, 2011
		RAFALOVITCH, "Viewfinder Friends-idea for Facebook application", November 14, 2007, http://blog.outerhoughts.com/2007/11/viewfinder-friends-idea-for-facebook-application/, 5pages.
		KISHORE, "How to Add, Upload, and Tag Your Pictures and Photos in FaceBook", http://www.online-tech-tips.com/fun-stuff/how-to-add-upload-and-tag-your-pictures-and-photos-in-facebook/, August 11, 2007, 13 pages.
		BECKER et al., "Evaluation of Face Recognition Techniques for Application to Facebook", IEEE International conference on Automatic Face and Gesture Recognition, 2008, 6 pages.
		BAKER, "Google & Riya Face Recognition Photo Search", November 22, 2005, http://www.searchenginejournal.com/google-riya-face-recognition-photo-search/25501, 1 page_
		PONCE, "Riya, Photo Sharing with Face Recognition", October 28, 2005, http://www.ohgizmo.com/2005/10/28/riya-photo-sharing-with-face-recognition/, 2 pages_
		FACEBOOK, "Making Photo Tagging Easier", https://m.facebook.com/notes/facebook/making-photo-tagging-easier/467145887130/?_tn_=C&_rdr, 2 pages
		MICHELSON et al., "Auto-tagging the Facebook", 2006, http://cs229.stanford.edu/proj2006/MichelsonOrtiz-AutoTaggingTheFacebook.pdf, 5 pages.
		ARRINGTON, "First Screen Shots of Riya", October 26, 2005, http://techcrunch.com/2005/10/26/riya-prepares-to-launch-alpha/, 10 pages
		ARRINGTON, "Ojos - Auto Name & Tag Your Photos", August 15, 2005, http://techcrunch.com/2005/08/31/ojos-auto-name-tag-your-photos/, 8 pages.
		STONE, et al. "Autotagging Facebook: Social network context improves photo annotation," In Workshop on Internet Vision, 2008, 2 pages_
		SCHUON et al., "CS229 Project Report: Automated photo tagging in Facebook", December 2007, http://cs229.Stanford.edu/proj2007/SchuonRobertsonZou-AutomatedPhotoTaggingInFacebook.pdf, 5 pages.
		YADAV, "Facebook - The Complete Biography", August 25, 2006, http://mashable.com12006/08/25/facebook-protile/, 7 pages_
		UNKNOWN, "What does it mean to "tag" someones picture on facebook, whats the point of doing it?", November 28, 2007, https://answers.yahoo.com/question/index?qid=20071128123629AAY0DLP, 2 pages.
		Yang, et al., "Detecting Faces in Images: A Survey", January 2002, IEEE Trans. Pattern Analysis Machine Intelligence, 24(1), 2 pages

EXAMINER	DATE CONSIDERED

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

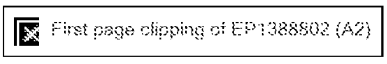
Espacenet

Bibliographic data: EP1388802 (A2) — 2004-02-11

Face identification device and face identification method

Inventor(s):	TAKENAKA HIDEKI [JP] ± (TAKENAKA, HIDEKI)
Applicant(s):	OMRON TATEISI ELECTRONICS CO [JP] ± (OMRON CORPORATION)
Classification:	**- international:** ***G06K9/00; G06T1/00; G06T5/00; G06T5/20; G08B13/196; G08B15/00; H04N7/18;*** (IPC1-7): G06K9/00; G06T3/00; G08B13/196 **- cooperative:** **G06K9/00221**; **G06T5/002**; **G08B13/1961**; **G08B13/19686**; G06T2207/30201
Application number:	EP20030016612 20030729
Priority number (s):	JP20020220655 20020730
Also published as:	EP1388802 (A3) EP1388802 (B1) AT394751 (T) CN1472691 (A) JP2004062560 (A) more

Abstract of EP1388802 (A2)



The present invention is to protect the right of portrait or privacy of people (10B to 10F) other than a specific person (10A), and to enable easy recognition of information other than the face (11) of the specific person (10A) and the situation around the specific person (10A). Images videotaped by the surveillance cameras (1) are captured in the computer (3), face images are detected therefrom, and the detected face images are compared with the face image of a specific person (10A) registered in the storage device (5).; As the results of the comparison, when these face images do not match with each other, a mosaic process (12) is applied exclusively to the detected face images to protect the privacy of the people (10B to 10F) other than the specific person (10A), whereas the mosaic process (12) is not applied to the parts other than the faces, such as dress and baggage, thereby keeping them as they are. When these face images match with each other, the face image of the specific person (10A) is not applied with the mosaic process (12), thereby keeping his or her face (11) and remaining parts as they are.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 388 802 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
11.02.2004 Bulletin 2004/07

(51) Int Cl.[7]: **G06K 9/00**, G06T 3/00, G08B 13/196

(21) Application number: **03016612.8**

(22) Date of filing: **29.07.2003**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR
Designated Extension States:
AL LT LV MK

(30) Priority: **30.07.2002 JP 2002220655**

(71) Applicant: **Omron Corporation**
Kyoto-shi, Kyoto 600-8530 (JP)

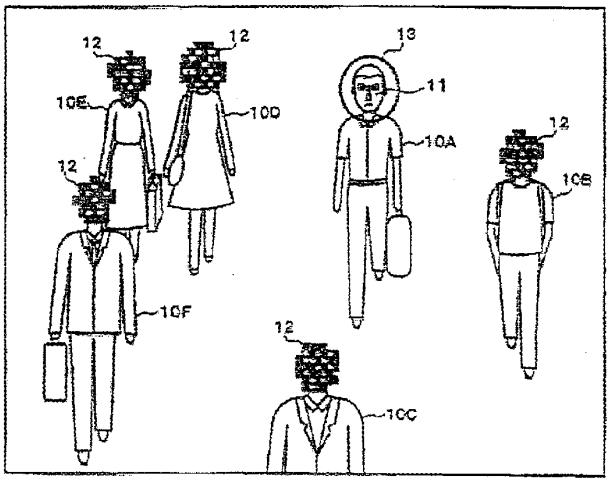
(72) Inventor: **Takenaka, Hideki, Omron Corp.**
801 Minamifudodo-cho
Kyoto-shi, Kyoto 600-8530 (JP)

(74) Representative: **Käck, Jürgen**
Kahler Käck Mollekopf
Patentanwälte
Vorderer Anger 239
86899 Landsberg (DE)

(54) Face identification device and face identification method

(57) The present invention is to protect the right of portrait or privacy of people (10B to 10F) other than a specific person (10A), and to enable easy recognition of information other than the face (11) of the specific person (10A) and the situation around the specific person (10A). Images videotaped by the surveillance cameras (1) are captured in the computer (3), face images are detected therefrom, and the detected face images are compared with the face image of a specific person (10A) registered in the storage device (5). As the results of the comparison, when these face images do not match with each other, a mosaic process (12) is applied exclusively to the detected face images to protect the privacy of the people (10B to 10F) other than the specific person (10A), whereas the mosaic process (12) is not applied to the parts other than the faces, such as dress and baggage, thereby keeping them as they are. When these face images match with each other, the face image of the specific person (10A) is not applied with the mosaic process (12), thereby keeping his or her face (11) and remaining parts as they are.

Fig. 5



EP 1 388 802 A2

Printed by Jouve, 75001 PARIS (FR)

Description

BACKGROUND OF THE INVENTION

Technical Field

[0001] The present invention relates to a face identification technique which detects human faces from images taken by a camera and compares themwith a previously registered face, thereby detecting a specific person.

Related Background Art

[0002] In order to search for a specific person like a criminal on the wanted list, such a system is available that videotapes an unspecified number of the general public and records their images by installing surveillance cameras in airports, stations, shopping centers, busy streets, and the like. In this system, videotaped images are recorded as they are or face images are exclusively recorded by being extracted from the videotaped images. In these methods, there is a problem that face images of the people other than the specific person are also recorded, failing to protect their rights of portrait or privacy.

[0003] Therefore, there is a system now available, according to which the face image of a person videotaped by a surveillance camera is compared with the face image of the specific person registered: the face image of a videotaped person is recorded if these face images match with each other, whereas when these face images do not match with each other, the face image of the videotaped person is abandoned. In this system, out of the face images videotaped, those which do to match with the face image of the registered specific person are not kept, thereby securing protection of their privacy.

[0004] However, in the above-described system, what is recorded is only the face image matching with the face image of the specific person, and other useful information including the dress and baggage of the specific person and the situation around him or her are lost. As a result, when there is a match and a responsible official rushes to the display monitor by a report or when recorded images are confirmed later, the absence of information other than his or her face makes it difficult to search for the specific person.

[0005] On the other hand, in order to protect individuals' privacy, there is an approach of applying a mosaic process on face images as described in Japanese Laid-Open Patent Application No. 2001-86407. However, in this patent application, skin color is detected from videotaped human images and a mosaic process is automatically applied to face images, which forces all face images videotaped to be applied with a mosaic process, thereby making it impossible to apply a mosaic process to the face images excluding the face image of the specific person.

[0006] Japanese Laid-Open Patent Application No. 2000-216 also discloses privacy protection measures by applying a mosaic process to human body images. However, when the technique of this patent application is used to protect the privacy of the people other than the specific person, it is difficult to check the situation around the specific person, because the whole image of the specific person is applied with the mosaic process.

DISCLOSURE OF THE INVENTION

[0007] The present invention, which is intended to solve the aforementioned problems, has the object of facilitating confirmation of information other than the face of a specific person and situation around the specific person, while protecting the right of portrait or privacy of the people other than the specific person.

[0008] The face identification device of the present invention comprises: detection means for detecting face images from human body images taken by a camera; storage means in which a face image of a specific person is previously stored; determination means for determining whether a face image detected by the detection means matches with the face image stored in the storage means by comparing both face images; and abstraction means for applying an abstraction process to a predetermined face image out of the face images detected by the detection means in order to make the predetermined face image unrecognizable. The abstraction means applies the abstraction process exclusively to a detected face image when the determination means determines that both face images do not match with each other. On the other hand, the abstraction means does not apply the abstraction process to a detected face image when the determination means determines that both face images match with each other.

[0009] The face identification method of the present invention comprises the steps of: detecting face images from human body images taken by a camera; determining whether a detected face image matches with the face image previously stored by comparing both face images; applying an abstraction process exclusively to a detected face image in order to make the detected face image unrecognizable, when it is determined that both face images do not match with each other; and not applying the abstraction process to the detected face image when it is determined that both face images match with each other.

[0010] The term "match" referred to in the above description means not only a complete match between a detected face image and the face image previously stored, but also a high degree of resemblance between these face images.

[0011] According to the present invention, when a detected face image and the registered face image do not match with each other, that is, when the detected face does not belong to the specific person, an abstraction

process is applied on the face image in order to protect the right of portrait or privacy of the people other than the specific person. Furthermore, the abstraction process is applied only to the face images of the people, keeping images other than their faces, such as their dress and baggage. On the other hand, when a detected face image and the registered face image match with each other, that is, when the detected face belongs to the specific person, both the face image and images including the dress and baggage of the specific person are kept without being applied with the abstraction process. Thus keeping the images for the dress and baggage of a specific person and of the other people as they are can facilitate the search for the specific person by using these images as an important clue.

[0012] A typical example of the abstraction process in the present invention is a mosaic process. The use of the well-known mosaic process can abstract face images easily. Besides the mosaic process, various other methods are available for abstraction, such as blurring or filling in face image portions.

[0013] In the present invention, when it is determined that a detected face image matches with the stored face image, a marker is applied to the detected face image portion instead of applying an abstraction process thereto. The application of a marker makes a specific person distinguishable at a glance.

[0014] In the present invention, when it is determined that a detected face image matches with the stored face image, the image of the specific person applied with the abstraction process neither to his or her face nor remaining parts and the images of the other people applied with the abstraction process exclusively to their faces are displayed. At the same time, a warning is outputted. This system realizes a quick response because the warning is outputted at the time of the detection of a specific person. Concerning a specific person, the videotaped image is displayed as it is, and as for the people other than the specific person, the abstraction process is applied to their faces to protect their privacy while the images of their dress and baggage are displayed as they are. This makes it possible to obtain useful information about the specific person and the situation around him or her, thereby facilitating the search for the specific person.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015]

Fig. 1 shows a block diagram of the face identification system to which the present invention is applied.

Fig. 2 shows a flowchart depicting the procedure for registering face images.

Fig. 3 shows a flowchart depicting the procedure of the face identification method of the present invention.

Fig. 4 shows a flowchart depicting a specific procedure of identification.

Fig . 5 shows an image example to which mosaic process has been applied.

Fig. 6 shows a flowchart depicting the identification procedure in the case where a face image is registered afterwards.

Fig. 7 shows a flowchart depicting another embodiment of the face identification method.

Fig. 8 shows a flowchart depicting the identification procedure in the case where a face image is registered afterwards in another embodiment.

Fig. 9 shows a block diagram showing another embodiment of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0016] Fig. 1 shows a block diagram of the face identification system to which the present invention is applied. In the drawing, the face identification system is composed of surveillance cameras 1 for videotaping the images of people, and the face identification device 2 of the present invention for identifying face images of the people videotaped by the surveillance cameras 1. Aplural number of the surveillance cameras 1 are installed in airports, stations, shopping centers, busy streets, and other places where a number of people gather, and each of the cameras 1 is connected with the face identification device 2 installed in a monitor center or the like.

[0017] In the face identification device 2, reference numeral 3 is a computer for face identification; reference numeral 4 is an identification results output device for outputting the results of face identification by the computer 3; and reference numeral 5 is a storage device which previously stores the face image data of a specific person (e.g., a suspect on the wanted list). Reference numerals 6 and 7 are image input devices for registering a face image to the storage device 5: reference numeral 6 is a scanner and reference numeral 7 is a digital camera. The computer 3 includes detection means for detecting face images from images of people videotaped by the surveillance cameras 1; determination means for determining the presence or absence of a match between a detected face image and the face image stored in the storage device 5 by comparing them; and abstraction means for applying an abstraction process to a predetermined face image out of the detected face images so as to make the face unrecognizable. The identification results output device 4 is composed of a display monitor for displaying identification results, a printer for printing identification results, and other output devices. The storage device 5 can be a hard disk or the like, which composes the storage means of the present invention. Besides a hard disk, an optical disk can be used as the storage means.

[0018] Operation of the face identification system having the above-explained structure will be described as follows. In this system, the face image of a specific

person is previously registered in the storage device 5. Fig. 2 shows a flowchart depicting the procedure of face image registration, which is executed by the computer 3. At first, an image including the face of a specific person to be registered is captured into the computer 3 from the scanner 6 or the digital camera 7 (Step S1). Next, the face to be registered is detected from the captured image (Step S2). This face detection can be done by using a well-known approach, such as skin color detection, abstraction of difference with a background image, or abstraction of face likelihood from pattern matching. After the face detection, featuring points such as eyes, nose, mouth, and ears are detected from the face image (Step S3) , and the amount of feature about the shape and position of each detected featuring point is extracted (Step S4). This abstraction of feature amount also can be done by using a well-known approach, such as extraction of the amount of feature from gray-scale images including eyes, nose, mouth, and ears by template matching. The amount of feature extracted is stored and registered in the storage device 5 as face image data (Step S5).

[0019] Fig. 3 shows a flowchart depicting the procedure of the face identification method of the present invention, the procedure being executed by the computer 3. In the computer 3 , images videotaped by the surveillance cameras 1 are captured as still images at the interval of e.g. one second (Step S11), and human faces are detected from the captured images (Step S12). If there is no face detected (Step S13:NO), the process goes back to Step S11 and captures images in the next timing. If a face is detected (Step S13:YES), the detected face image is compared with the face image previously registered in the storage device 5 (Step S14) so as to determine whether or not these face images match with each other (Step S15).

[0020] Fig. 4 shows a flowchart depicting the specific procedure of the comparison in Step S14 . In the comparison, featuring points (eyes, nose, mouth, and the like) are detected from the detected face image (Step S31), and the amount of feature about the shape and position of each detected featuring point is extracted (Step S32). The extracted amount of feature is compared with the amount of feature of the face registered in the storage device 5 (Step S33). Based on the comparison results, it is determined whether these face images match with each other or not at Step S15 shown in Fig. 3. The term "match" referred to in this case means not only a complete match, but also a high degree of resemblance between these face images. To be more specific, the degree of resemblance is calculated from the amount of feature of each face image, and is compared with a predetermined threshold value. When the degree is equal to or over the threshold value, it is determined as a match.

[0021] As the results of the determination at Step S15, when a detected face image and the registered face image do not match with each other (Step S15:NO), the detected face image does not belong to the specific person registered. Therefore, the mosaic process is applied to the detected face image portion (Step S16). Fig. 5 shows an example of images to which the mosaic process has been applied: the mosaic process 12 is applied to each face image of the persons 10B to 10F except the specific person so as to abstract their faces unrecognizably. The mosaic process 12 is applied exclusively to the face image portions, keeping dress and baggage portions unprocessed.

[0022] On the other hand, when a detected face image matches with the registered face image (Step S15: YES), it means that the detected face image belongs to the registered specific person, so a marker is applied to the detected face image portion instead of applying the mosaic process thereto (Step S17). In Fig. 5, the person 10A is the specific person, and the mosaic process 12 is not applied to the face image portion of the specific person 10A, thereby keeping the face 11 the same as when it is videotaped by the surveillance cameras 1. The face 11 is enclosed by the marker 13 to make the specific person distinguishable at a glance. The mosaic process 12 is not applied to the dress or baggage of the specific person 10A. In other words, concerning the specific person 10A, the image videotaped by the surveillance cameras 1 appears as it is.

[0023] After the process in Step S17, the identification results output device 4 displays, with a warning, the images shown in Fig. 5 including the image of the specific person 10A whose face and remaining parts are not applied with the mosaic process 12, and the images of the persons 10B to 10F whose faces are exclusively applied with the mosaic process (Step S18). This warning is displayed as a message including the name of the specific person, the time and date of the image videotaped, and the place videotaped. Furthermore, an alarm is issued as necessary with the display in order to draw the responsible official's attention. This enables the official to prepare the deployment of members for the search for the specific person.

[0024] Since the faces of the people other than the specific person 10A are applied with the mosaic process 12 as shown in Fig. 5, when the images are displayed on the display monitor, there is no fear of violating their rights of portrait or privacy. Furthermore, the mosaic process 12 is applied exclusively to their faces, keeping the remaining parts unprocessed, which enables easy recognition of the dress and baggage of the people around the specific person 10A. On the other hand, concerning the specific person 10A, the videotaped image of the whole body appears as it is, making it possible to confirm his dress and baggage in addition to his face. Thus, the mosaic process 12 is applied exclusively to face portions which raise the issue of privacy, and the remaining parts are kept the same as when they are videotaped, thereby facilitating the search for the specific person 10A by using the dress and baggage as a useful clue.

[0025] After Steps S16 to S18 are executed, it is determined whether matching is done for all the detected faces (Step S19). When there is still a face to be checked (519:NO) the process goes back to Step S14 to check the next face. When all the detected faces have been checked (S19:YES) , the image to which the procedure of Steps S16 and S17 has been applied is recorded to the storage device 5 (Step S20). Later, the process goes back to Step S11, and videotaped images are captured from the surveillance cameras 1 again in the next timing (in one second in this case) . Hereafter, the procedure in Steps S12 to S20 is repeated.

[0026] The above example describes the case where images videotaped by the surveillance cameras 1 are captured as still images at the interval of one second; however, it is also possible to adopt a system which detects human faces from motion images videotaped by the surveillance cameras 1 and checks the faces while automatically chasing them. In this system, there is no need for the repeated recording of the image of the same person, which can reduce the amount of image data to be recorded in the storage device 5, thereby enabling miniaturization of the storage device 5.

[0027] Images stored in the storage device 5 can be outputted by being displayed or printed by the identification results output device 4 later at any point in time. In this case, too, the privacy of the people other than the specific person 10A is protected by applying the mosaic process to their faces, whereas the images for the dress and baggage including those of the specific person are stored as they are. This information can be used as a clue to facilitate the search for the specific person 10A.

[0028] In the aforementioned embodiment, the face image of a specific person is previously registered, and face images videotaped by surveillance cameras are compared with the registered face image so as to detect the specific person; however, it is also possible to detect a specific person registered afterwards by using images stored in the storage device 5. This system enables the detection of people whom the police has been requested to find or stray children.

[0029] Fig. 6 shows a flowchart depicting the procedure of identification in the case of registering afterwards as described above, the procedure being executed by the computer 3 . At first, images stored in the storage device 5 are captured by the computer 3 (Step S41). The images stored in the storage device 5 are unrecognizable because of the above-described mosaic process, so it is necessary to reconstruct the original images for comparison. Therefore, the mosaic process is cleared to reconstruct the original images (Step S42). After the reconstruction of the original images, faces are detected from the reconstructed images (Step S43) . If no face is detected from the reconstructed images (Step S44:NO), the process goes back to Step S41 to capture recorded images. On the other hand, if faces are detected from the reconstructed images (Step S44:YES), detected face images are compared with the face image which is registered afterwards (Step S45). The face image registered afterwards is taken by the scanner 6 or the digital camera 7 and recorded to the storage device 5 in the same manner as the previously registered case.

[0030] If the comparison results in Step S45 indicate that a recorded image face does not match with the face registered afterwards (Step S46:NO), it is determined whether all faces detected from the recorded images have been checked or not (Step S47). When there is a face left unchecked (Step S47:NO), the process goes back to Step S45 to check the next face. When all faces have been checked (Step S47:YES), it is determined whether all the recorded images have been checked or not (Step S48). If all recorded images are not checked (Step S48:NO), the process goes back to Step S41 to capture the next recorded image from the storage device 5 and the aforementioned procedure is repeated. When the comparison for all recorded images is complete (Step 548:YES), the absence of the face image matching with the face image registered afterwards is reported by being displayed on the display monitor of the identification results output device 4 (Step S49).

[0031] On the other hand, in Step S46, if a recorded face image matches with the face registered afterwards (Step S46:YES), the reconstructed original image is outputted to the identification results output device 4 and shown on the display monitor (Step S50). And it is reported by being shown on the display monitor that there is a recorded face image which matches with the face registered afterwards (Step S51).

[0032] In the comparison in the above-described case where a face image is registered afterwards, it is preferable in terms of security that the process for reconstructing original images by clearing the mosaic process applied to images stored in the storage device 5 can be done exclusively by an authorized person (e.g., system administrator). Figs. 7 and 8 show flowcharts depicting the embodiment of this case.

[0033] Fig. 7 shows a flowchart corresponding to the flowchart shown in Fig. 3, so the same steps as those in Fig. 3 are referred to with the same symbols. The procedure in Steps S11 to S19 is the same as in Fig.3, so its explanation is omitted. When all faces have been checked in Step S19 (Step S19:YES), the face image of a recorder who records images is captured (Step S20a); the captured face image of the recorder is embedded as a "digital watermark" in the images processed in Steps S16 and S17; and the images with the "digital watermark" are stored in the storage device 5 (Step S20b) . The term "recorder" used in this case can be a system administrator, and the face image of the recorder which is captured in Step S20a is previously taken by the scanner 6 or the digital camera 7 and stored in the storage device 5.

[0034] The following is a description on the procedure for reconstructing original images. Fig. 8 shows a flowchart corresponding to the flowchart of Fig. 6, so the same steps as those in Fig. 6 are referred to with the

same symbols. First, images stored in the storage device 5 are captured in the computer 3 (Step S41). Next, the face image of the operator who performs a reconstructing operation of images is captured (Step S41a). The face image of this operator is taken by the scanner 6 or the digital camera 7 at this point in time. Then, it is determined whether the face image data captured in Step S41a matches with the data of "digital watermark" embedded in the images captured in Step S41 or not (Step S41b). If these pieces of data do not match with each other (Step S41b:NO), it is determined that the operator who is going to perform the reconstructing operation is not the above-mentioned recorder (systemadministrator), and the process is terminated. On the other hand, when these pieces of data match with each other (Step S41b:YES), it is determined that the operator and the recorder (system administrator) are the same person, and the mosaic process is cleared to reconstruct the original images (Step S42). Since the procedure from Step S42 onward is equal to the procedure in Fig. 6, the explanation will be omitted.

[0035] As described hereinbefore, using the face image of the recorder as a "digital watermark" makes it possible to authorize only the recorder to perform reconstruction and to prohibit an unauthorized third party from clearing a mosaic process to reconstruct original images, thereby securing the security.

[0036] The present invention can adopt various other embodiments besides the embodiment described above. For example, in the above embodiment, a mosaic process is taken as an example of the abstraction process to be applied to face images; however, it is also possible to apply a process to blur face image portions, instead of applying the mosaic process. Alternatively, face image portions can be filled in black or white, instead of being applied with the mosaic process or the blurring process.

[0037] In the above embodiment, images which are videotaped by the surveillance cameras 1 and applied with a mosaic process or a marker are stored in the storage device 5; however, the images can be merely displayed on the display monitor of the identification results output device 4. In this case, there is no need for storage to the storage device 5.

[0038] In the above embodiment, face images which are registered either previously or afterwards are stored in the storage device 5, and images which are videotaped by the surveillance cameras 1 and applied with a mosaic process or a marker are also stored in the same storage device 5. Alternatively, as shown in Fig. 9, a special image storage device 8 can be provided in addition to the storage device 5 so that face images to be registered can be stored in the storage device 5 whereas images videotaped by the surveillance cameras 1 can be stored in the image storage device 8. The image storage device 8 can be composed of any kind of device dealing with recording media such as a video tape recorder, a DVD (Digital Versatile Disk) recorder, or a hard disk recorder. In that case, faces other than the face of the specific person are applied with an abstraction process, so there is no fear of violating their rights of portrait or privacy during reproduction.

[0039] According to the present invention, an abstraction process is applied exclusively to the face images of the people other than a specific person, thereby protecting their rights of portrait or privacy, whereas the images for the dress and baggage of the specific person and the other people are kept as they are. This information can be used as a clue to facilitate the search for the specific person.

Claims

1. A face identification device (2) comprising:

   detection means for detecting face images from human body images taken by a camera;
   storage means in which a face image of a specific person (10A) is previously stored;
   determination means for determining whether a face image detected by said detection means matches with the face image stored in said storage means by comparing both face images; and
   abstraction means for applying an abstraction process to a predetermined face image out of the face images detected by said detection means in order to make the predetermined face image unrecognizable,
   said abstraction means applying the abstraction process exclusively to a detected face image when said determination means determines that both face images do not match with each other, and not applying the abstraction process to a detected face image when said determination means determines that both face images match with each other.

2. The face identification device (2) according to claim 1, wherein said abstraction process is a mosaic process (12) for making a face image portion mosaic.

3. The face identification device (2) according to claim 1 or 2, wherein when said determination means determines that both face images match with each other, a detected face image is not applied with the abstraction process and is applied with a marker (13).

4. The face identification device (2) according to any one of claims 1 to 3 , wherein when a face image detected by said detection means is determined to match with the face image stored in said storage means, the image of the specific person (10A)

which is not applied with the abstraction process on the face (11) and remaining parts thereof and the images of people (10B to 10F) other than the specific person (10A) which are applied with the abstraction process exclusively on the faces thereof are displayed, and a warning is also outputted.

5. A face identification method comprising the steps of:

detecting face images from human body images taken by a camera;
determining whether a detected face image matches with the face image previously stored by comparing both face images;
applying an abstraction process exclusively to a detected face image in order to make the detected face image unrecognizable, when it is determined that both face images do not match with each other; and
not applying the abstraction process to the detected face image when it is determined that both face images match with each other.

Fig. 1

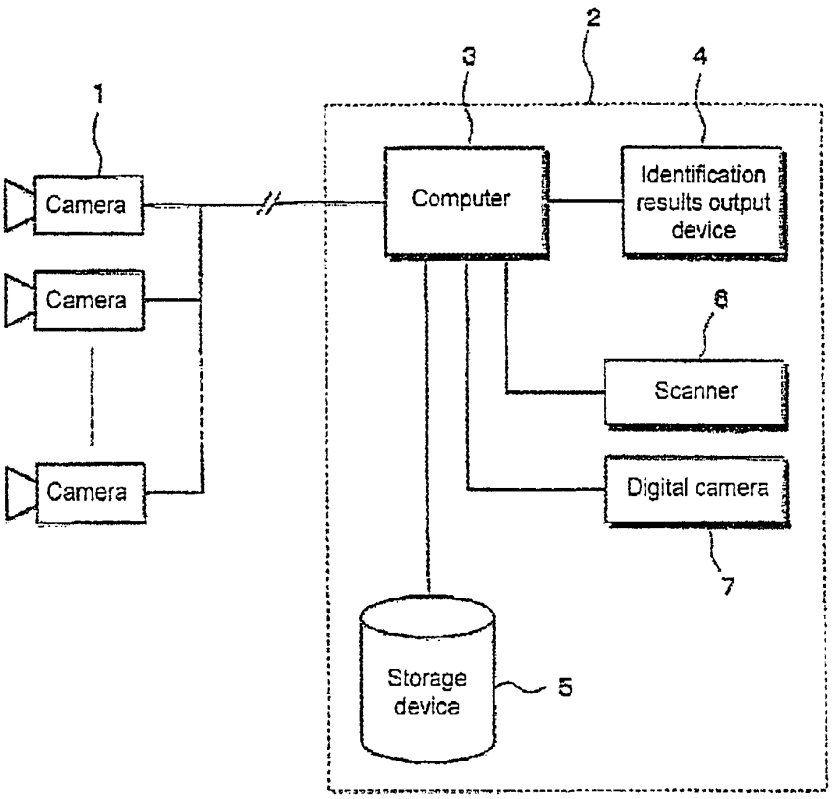

1
2
3
4
Camera
Camera
Camera
Computer
Identification results output device
6
Scanner
Digital camera
7
Storage device
5

Fig. 2

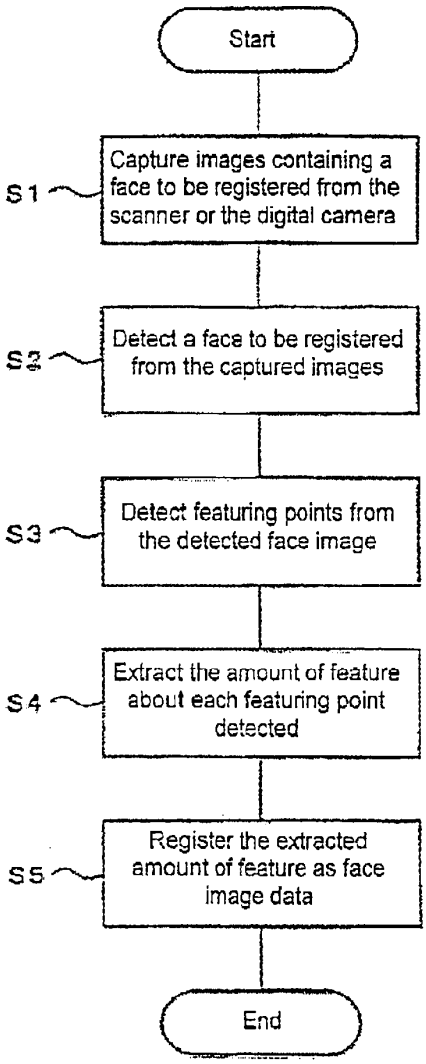

Start
S1
Capture images containing a face to be registered from the scanner or the digital camera
S2
Detect a face to be registered from the captured images
S3
Detect featuring points from the detected face image
S4
Extract the amount of feature about each featuring point detected
S5
Register the extracted amount of feature as face image data
End

Fig. 3

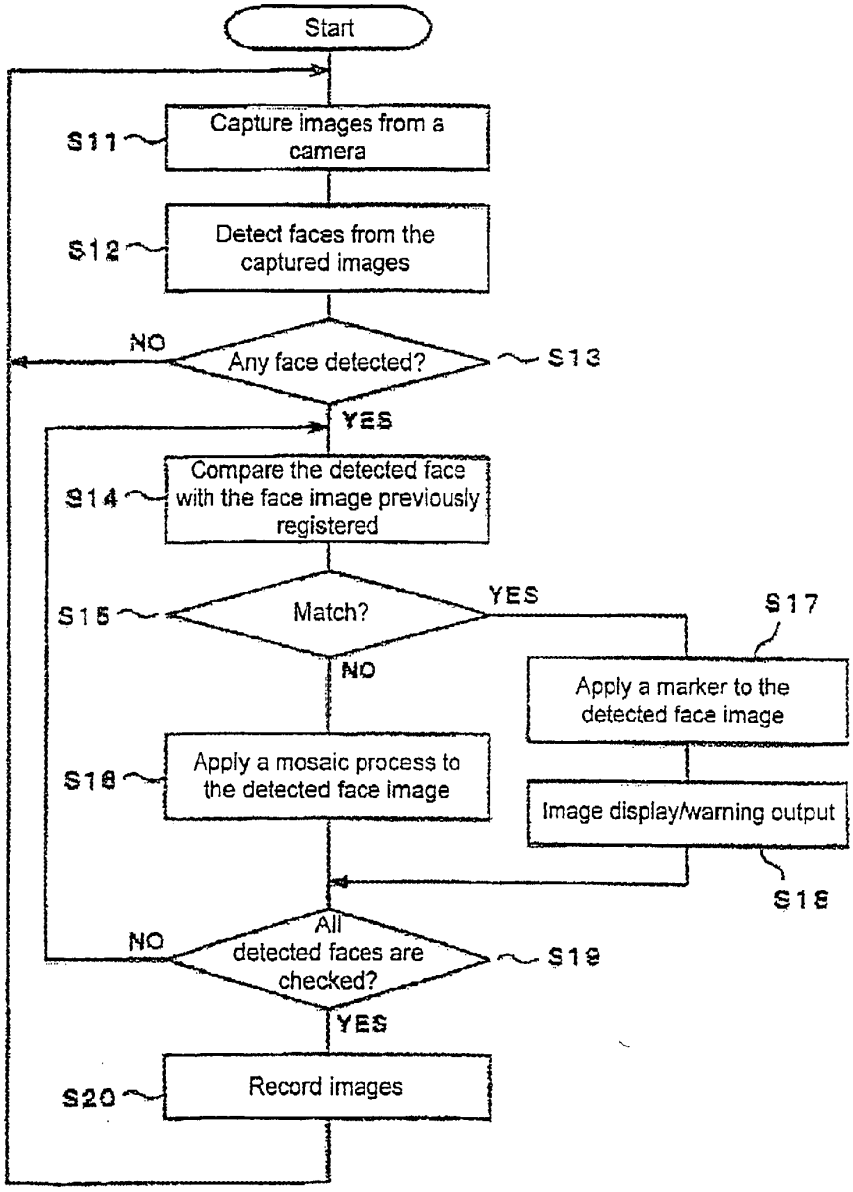

Start
S11
Capture images from a camera
S12
Detect faces from the captured images
NO
Any face detected?
S13
YES
S14
Compare the detected face with the face image previously registered
S15
Match?
YES
S17
NO
Apply a marker to the detected face image
S16
Apply a mosaic process to the detected face image
Image display/warning output
S18
NO
All detected faces are checked?
S19
YES
S20
Record images

Fig. 4

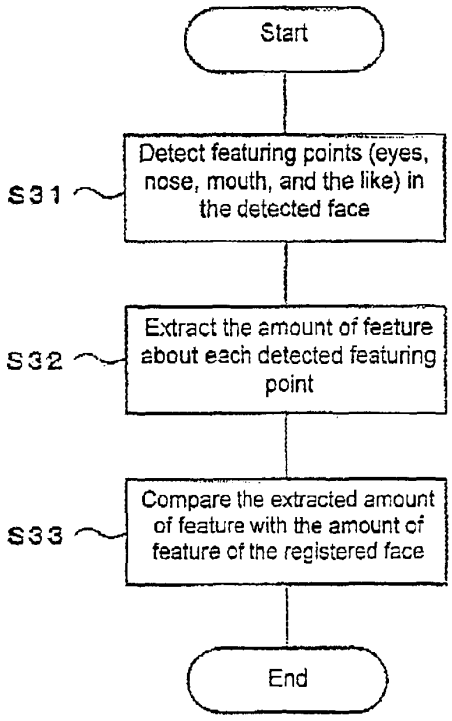

Start
S31
Detect featuring points (eyes, nose, mouth, and the like) in the detected face
S32
Extract the amount of feature about each detected featuring point
S33
Compare the extracted amount of feature with the amount of feature of the registered face
End

Fig. 5

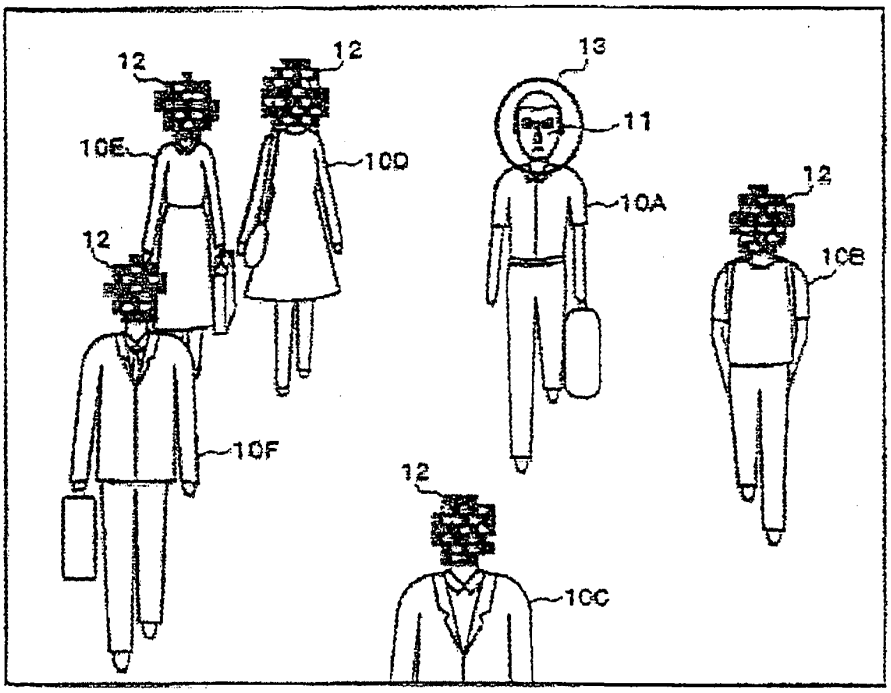


Fig. 6

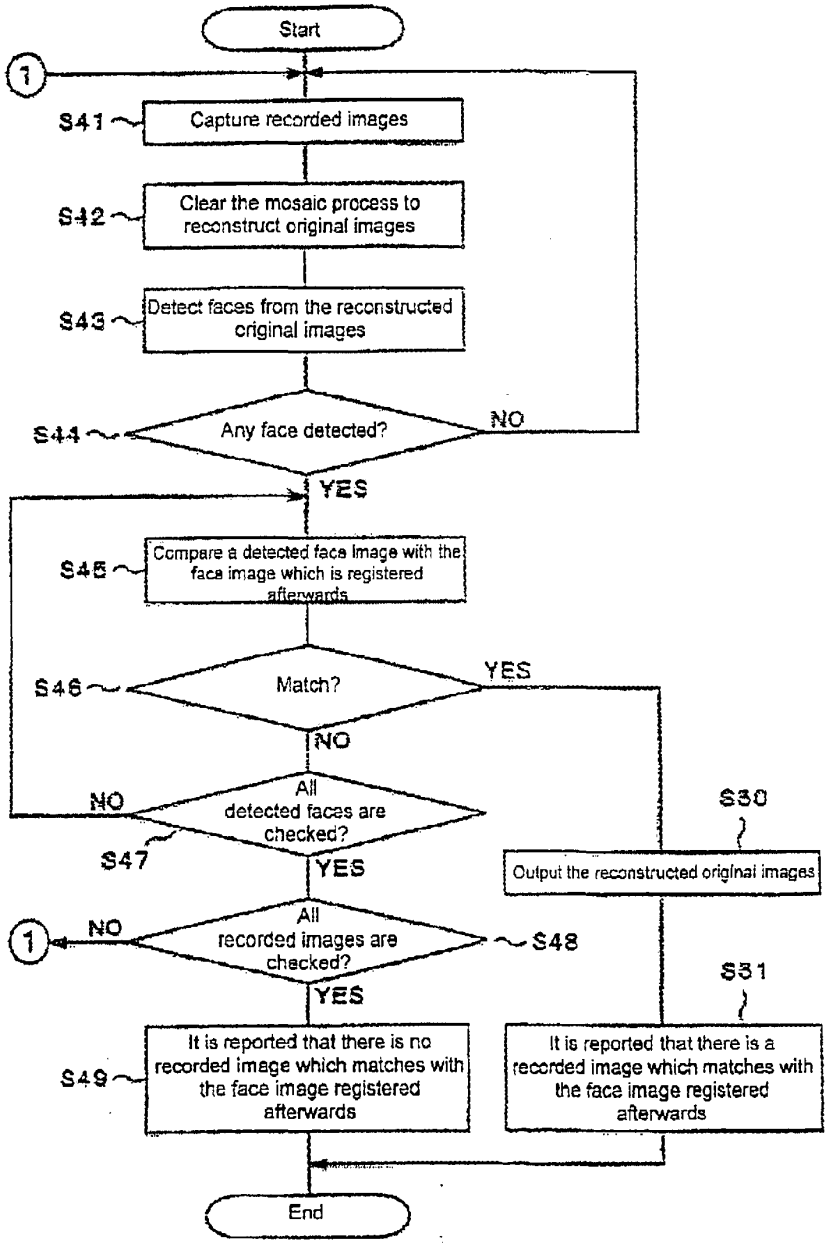

Start
1
S41
Capture recorded images
S42
Clear the mosaic process to reconstruct original images
S43
Detect faces from the reconstructed original images
S44
Any face detected?
NO
YES
S45
Compare a detected face image with the face image which is registered afterwards
S46
Match?
YES
NO
NO
All detected faces are checked?
S47
YES
S30
Output the reconstructed original images
1
NO
All recorded images are checked?
S48
YES
S31
S49
It is reported that there is no recorded image which matches with the face image registered afterwards
It is reported that there is a recorded image which matches with the face image registered afterwards
End

Fig. 7

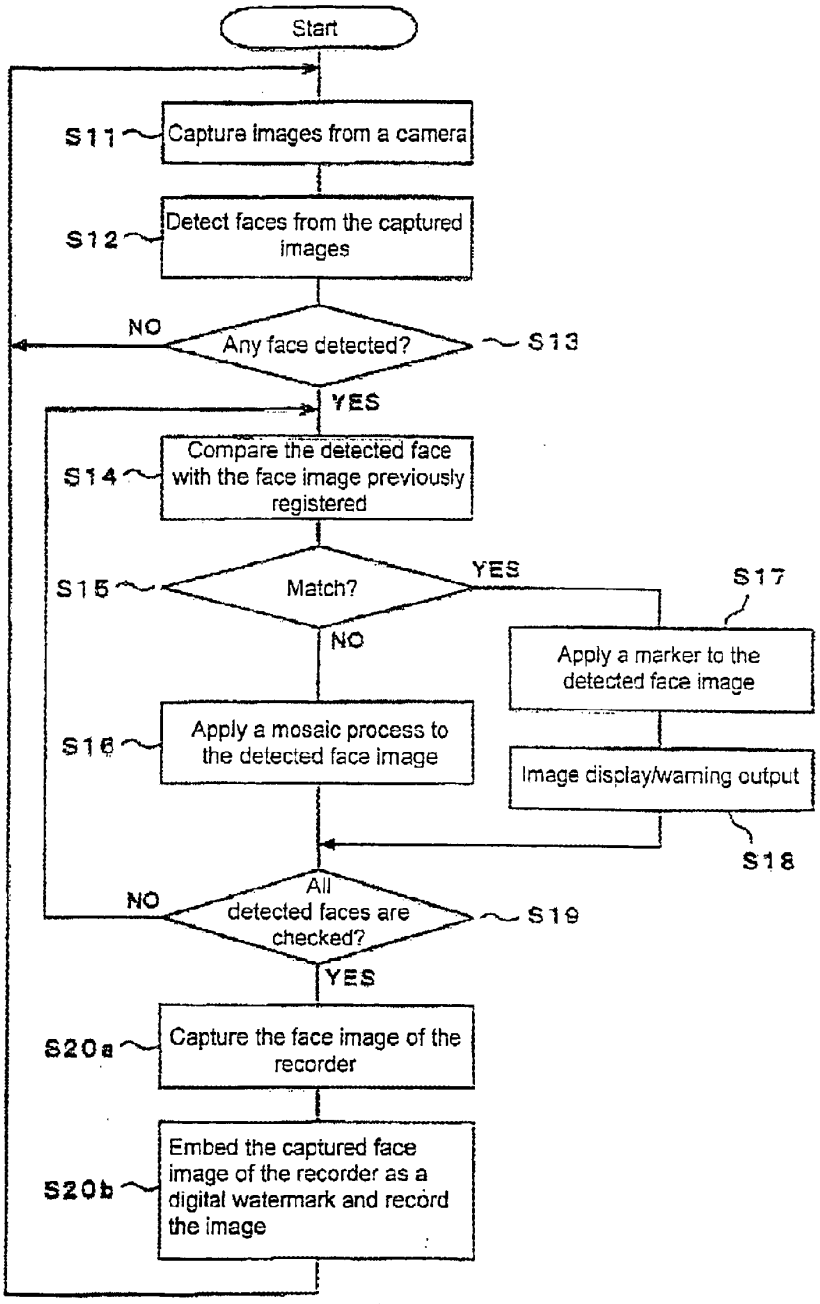

Start
S11
Capture images from a camera
S12
Detect faces from the captured images
NO
Any face detected?
S13
YES
S14
Compare the detected face with the face image previously registered
S15
Match?
YES
S17
Apply a marker to the detected face image
NO
S16
Apply a mosaic process to the detected face image
Image display/warning output
S18
NO
All detected faces are checked?
S19
YES
S20a
Capture the face image of the recorder
S20b
Embed the captured face image of the recorder as a digital watermark and record the image

Fig. 8

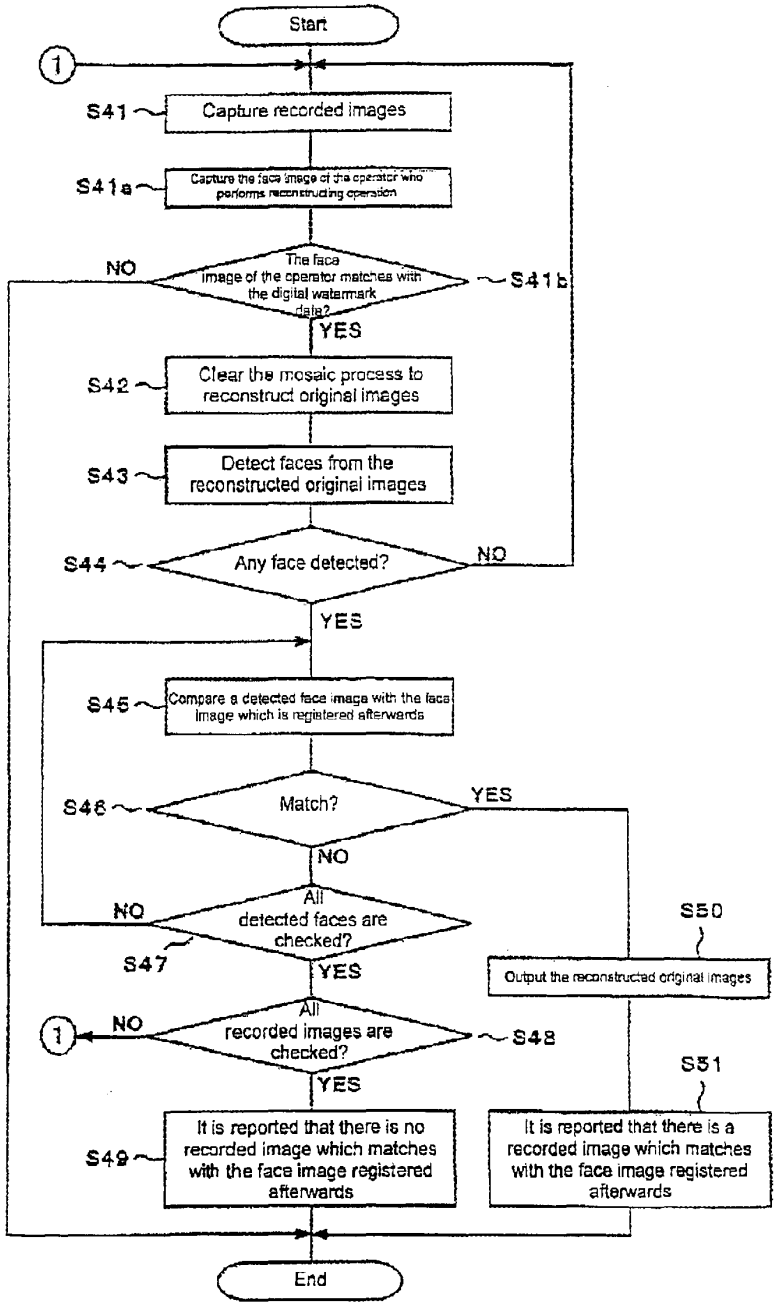
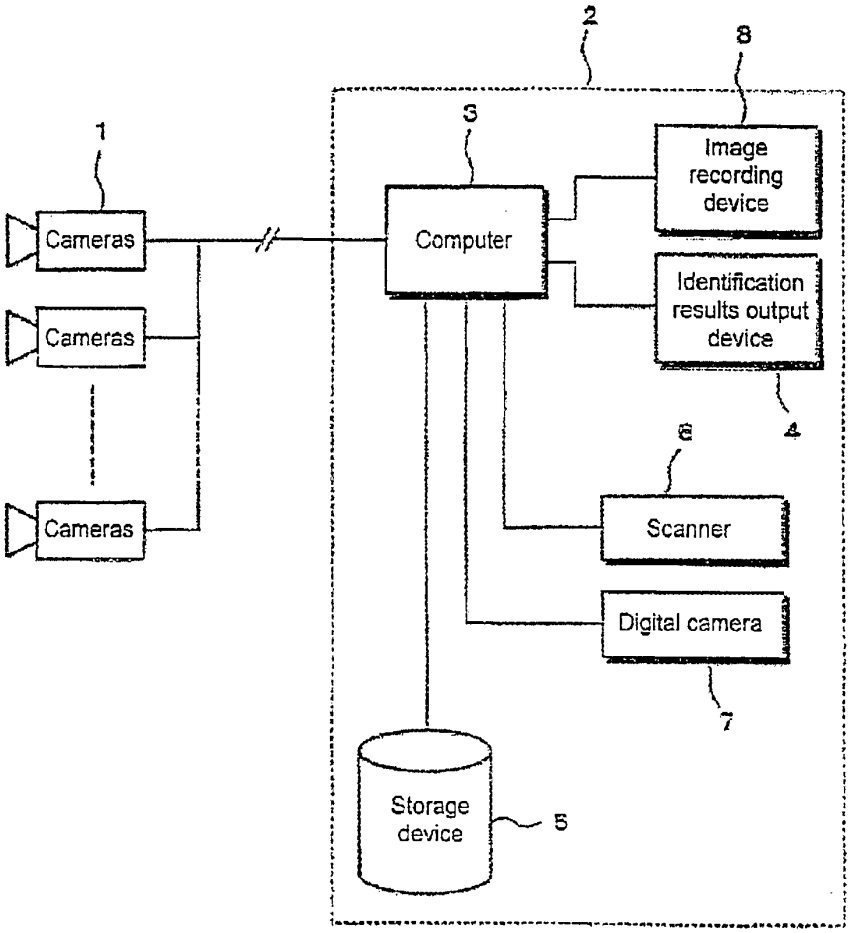

Start
1
S41
Capture recorded images
S41a
Capture the face image of the operator who performs reconstructing operation
NO
The face image of the operator matches with the digital watermark data?
S41b
YES
S42
Clear the mosaic process to reconstruct original images
S43
Detect faces from the reconstructed original images
S44
Any face detected?
NO
YES
S45
Compare a detected face image with the face image which is registered afterwards
S46
Match?
YES
NO
NO
All detected faces are checked?
S47
YES
S50
Output the reconstructed original images
1
NO
All recorded images are checked?
S48
YES
S51
S49
It is reported that there is no recorded image which matches with the face image registered afterwards
It is reported that there is a recorded image which matches with the face image registered afterwards
End

Fig. 9


2
8
1
3
Image recording device
Cameras
Computer
Cameras
Identification results output device
4
6
Cameras
Scanner
Digital camera
7
Storage device
5

Espacenet

Bibliographic data: EP1455297 (A1) — 2004-09-08

Image detection system and method

Inventor(s):	LEE HYEOK-BEOM [KR] ± (LEE, HYEOK-BEOM)
Applicant(s):	SAMSUNG ELECTRONICS CO LTD [KR] ± (SAMSUNG ELECTRONICS CO., LTD)
Classification:	**- international:** ***G06K9/00; G06K9/62;*** (IPC1-7): G06K9/00; G06K9/62 **- cooperative:** **G06K9/00228**; **G06K9/6232**
Application number:	EP20040251267 20040304
Priority number (s):	KR20030023791 20030415 ; KR20030014105 20030306
Also published as:	EP1455297 (B1) US2004183951 (A1) US7359529 (B2) DE602004005520 (T2)

Abstract of EP1455297 (A1)

First page clipping of EP1455297 (A1)

An image detection system and method that can detect and capture an image at a monitored position as an analog video signal and convert the analog video signal into a digital video signal for enlargement, analysis and storage of detected face images therein. The system comprises a candidate area detection unit for comparing a colour difference signal level of the converted digital video signal with a reference range for detecting at least one skin colour candidate area. The system further comprises a control unit for outputting a zoom control signal to the image-capturing unit to capture enlarged images of each detected skin colour candidate area and a face detection unit for detecting a face video signal from the enlarged images.; A compression/recording unit is provided for then compressing and recording the detected face image video signal, and allowing a user to easily perform a search for a subject's face when searching recorded video data.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 455 297 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
08.09.2004 Bulletin 2004/37

(51) Int Cl.[7]: **G06K 9/00**, G06K 9/62

(21) Application number: **04251267.3**

(22) Date of filing: **04.03.2004**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL LT LV MK

(30) Priority: **15.04.2003 KR 2003023791**
06.03.2003 KR 2003014105

(71) Applicant: **Samsung Electronics Co., Ltd.**
Suwon-si Gyeonggi-do 442-742 (KR)

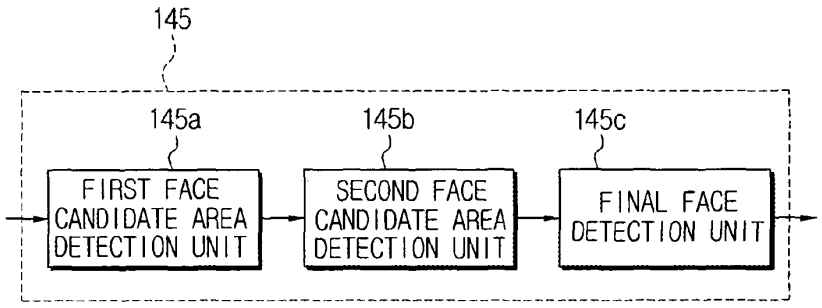
(72) Inventor: **Lee, Hyeok-beom**
Suwon-si Gyeonggi-do (KR)

(74) Representative: **Walaski, Jan Filip et al**
Venner Shipley LLP
20 Little Britain
London EC1A 7DH (GB)

(54) Image detection system and method

(57) An image detection system and method that can detect and capture an image at a monitored position as an analog video signal and convert the analog video signal into a digital video signal for enlargement, analysis and storage of detected face images therein. The system comprises a candidate area detection unit for comparing a colour difference signal level of the converted digital video signal with a reference range for detecting at least one skin colour candidate area. The system further comprises a control unit for outputting a zoom control signal to the image-capturing unit to capture enlarged images of each detected skin colour candidate area and a face detection unit for detecting a face video signal from the enlarged images. A compression/recording unit is provided for then compressing and recording the detected face image video signal, and allowing a user to easily perform a search for a subject's face when searching recorded video data.

FIG. 3



EP 1 455 297 A1

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] The present invention relates to an image detection system and method, particularly, but not exclusively, to a human face image detection system and method that is capable of detecting, enlarging and capturing face images, compressing the images for recordal and storage, and thereafter allowing search and retrieval of the compressed and recorded images.

[0002] The next generation closed-circuit TV (CCTV) system is a monitoring system having at least one monitoring camera installed at monitoring area where security is required, and a display for displaying the images taken by the installed monitoring camera in real time. The display is provided on monitors installed at certain places to enable fewer monitoring personnel to observe both usual and unusual situations at the monitoring areas.

[0003] Furthermore, the CCTV system records an image signal, such as a video signal taken through the monitoring system, on a recording medium, and reproduces and displays the recorded video signal on monitors. A digital video recorder (DVR) system is an example of one such CCTV system component.

[0004] The DVR system captures an analog video input signal from a monitoring camera, and compresses and records the analog video signal on a hard disc drive (HDD) as a high-definition digital video signal. Thus, the captured video signal can be recorded and maintained for a greater period without image quality deterioration, so that it can be used in cases that require evidence to be secured or searched for in the future.

[0005] A conventional CCTV system of this type uses at least one fixed monitoring camera to monitor and/or record positions where monitoring is necessary. However, the fixed monitoring camera is immobile, so that it captures images only for a specific area at the installed position, and often covers and captures images within a wide area rather than a specific, or narrower, part of the monitoring area. Accordingly, a video signal for the wide area suffers from poor image quality when compared to a video signal taken for a specific part of the monitoring area, causing difficulties in exactly identifying a subject within the image. Therefore, since the monitoring camera captures images of both the subject and the surroundings, rather than images specific to the subject in the monitoring area, the subject's face is recorded as relatively small, so that it is difficult to identify, which causes difficulties in securing clear identification evidence for future use.

[0006] Furthermore, the conventional CCTV system has a lower recording space efficiency level since it records all video signals taken of subjects and surroundings. Having recorded such a large amount of information, the conventional CCTV system requires a long time to search for a desired video signal.

[0007] Accordingly, a need exists for a monitoring system and method that is capable of detecting and recording face images from a monitored position, excluding surroundings, such that the images are more useful and the analysis, storage and retrieval of images is achieved in an efficient manner.

[0008] Therefore an object of the present invention is to provide a monitoring system and method for detecting and recording specific images, such as face images, from a monitored position and excluding surroundings from the images, such that the images are more useful for various purposes, such as identification.

[0009] Another object of the present invention is to provide a monitoring system and method for analysis, storage and retrieval of images in an efficient manner.

[0010] According to a first aspect of the invention, there is provided an image detection system comprising an image capture unit for capturing an image characterised by means for detecting a skin colour candidate area within the image and means responsive to detection of the skin colour candidate area to cause the image capture unit to capture an enlarged image of the skin colour candidate area.

[0011] According to a second aspect of the invention, there is provided a method of image detection, comprising capturing an image using an image capture unit, characterised by detecting a skin colour candidate area within the image and in response to detection of the skin colour candidate area, causing the image capture unit to capture an enlarged image of the skin colour candidate area.

[0012] According to a further aspect of the invention, there is provided a monitoring system and method that can detect and capture face images at a monitored position as an analog video signal, and in response, convert the analog video signal into a digital video signal for enlargement, analysis and storage of the face image. The monitoring system comprises a candidate area detection unit for comparing a colour difference signal level of the converted digital video signal with a predetermined reference colour difference signal level range, that is predetermined for a skin colour decision, and in response, detecting at least one skin colour candidate area.

[0013] The monitoring system further comprises a control unit for outputting a zooming control signal to the image-capturing unit to capture enlarged images of each detected skin colour candidate area. A conversion unit is provided for converting each skin colour candidate area captured in the enlarged image into an enlarged image digital video signal for use with a face detection unit for detecting a face video signal from the converted enlarged image digital video signal. A compression/recording unit is then provided for compressing and recording the detected face image video signal.

[0014] The system scans for candidate areas and once found, directs the capture of enlarged images. If a face image

is detected in these enlarged images, the enlarged face image is recorded for use. Accordingly, the system and method enables a user to easily perform a search for a subject's face when searching recorded video data.

[0015] The invention will be described in detail with reference to the following drawings in which like reference numerals refer to like elements, and wherein:

Figure 1 is a block diagram showing an example of a face image monitoring system according to an embodiment of the present invention;
Figure 2 is a block diagram showing an example of a candidate area detection unit of Figure 1 in detail;
Figure 3 is a block diagram showing an example of a face detection unit of Figure 1 in detail; and
Figure 4 is a flow chart illustrating an example of a face image detection method for a monitoring system as shown in Figure 1.

[0016] Hereinafter, the present invention will be described in detail with reference to the attached drawings.

[0017] Figure 1 is a block diagram showing an example of a face image monitoring system according to an embodiment of the present invention, Figure 2 is a block diagram showing an example of a candidate area detection unit of Figure 1 in detail and Figure 3 is a block diagram showing an example of a face detection unit of Figure 1 in detail.

[0018] Referring to Figure 1, an example of a face image monitoring system 100 according to an embodiment of the present invention has an image capture unit 105, also referred to as an image-photographing unit, a pan/tilt/zoom drive unit (hereinafter, referred to as "P/T/Z drive unit") 110, an analog to digital conversion unit (hereinafter referred to as "ADC") 115, a switching unit 120, a candidate area detection unit 125, a candidate area decision unit 130, a control unit 135, a candidate area storage unit 140, a face detection unit 145, a compression unit 150, a database (hereinafter, referred to as "DB") generation unit 155, a recording unit 160, a decompression unit 165, a digital to analog conversion unit (hereinafter referred to as "DAC") 170, and a key manipulation unit 175. A bus 180 is provided for coupling the control unit 135, compression unit 150, database generation unit 155, recording unit 160 and decompression unit 165.

[0019] The image capture unit 105 is a camera device, such as a charge coupled device (CCD) camera driven by the P/T/Z drive unit 110 to capture images of predefined monitoring areas. The CCD camera can pan in a horizontal direction, tilt in a vertical direction, zoom in and out, and output an analog video signal taken by the CCD camera. A plurality of image capture units 105 can be installed, each of which can have an identification number.

[0020] In the embodiment of the present invention shown in Figure 1, one image capture unit 105 is used to capture images of at least one monitoring area. However, in the case of two or more monitoring areas, the single image capture unit 105 can repeat image capturing operations at first one predefined monitoring area for a first predetermined period of time, and then move to a second monitoring area to capture images for a second predetermined period of time, and so on for any number of monitoring areas. For example, where the monitoring system 100 is installed in a bank and captures images of three bank windows through one image capture unit 105, the image capture unit 105 captures images of one bank window at a fixed state for a first predetermined period of time, moves to a position where it can capture images of the next bank window for a second predetermined period of time, and then moves to a position where it can capture images of the next teller's area for a third predetermined period of time. In this example, it is preferable that the first, second and third predetermined periods of time for capturing images of each teller's area are the same. However this can be configured as required by the application.

[0021] Returning to Figure 1, the P/T/Z drive unit 110 drives the image capture unit 105 based on driving control signals, for example, a zooming control signal, a pan/tilt position control signal, and so on, output from the control unit 135 described in greater detail below.

[0022] To do so, the P/T/Z drive unit 110 includes a zooming drive unit (not shown) for driving a zoom lens (not shown) to capture enlarged images of a candidate area based on a zooming control signal. The P/T/Z drive unit 110 further includes a pan/tilt drive unit (not shown) for driving the image capture unit 105 to move to positions where it can capture images of candidate areas based on a position control signal.

[0023] The ADC 115 converts the analog video signal provided by the image capture unit 105 into a digital video signal.

[0024] The switching unit 120 selectively provides the digital video signal output from the ADC 115 to either the candidate area detection unit 125 or the face detection unit 145, and is preferably implemented by a multiplexer. The switching unit 120 is configured to initially provide the digital video signal output from the ADC 115 to the candidate area detection unit 125. Further operation of the system 100 results in a digital video signal of an enlarged image area that is provided to the face detection unit 145 as described in greater detail below.

[0025] The candidate area detection unit 125 uses a colour difference signal provided by the digital video signal output from the switching unit 120 to detect at least one skin colour candidate area consisting of a colour difference signal similar to a colour difference signal for a human skin colour.

[0026] To do this, the candidate area detection unit 125 has a colour difference signal calculation unit 125a, a filter 125b, and a skin colour candidate area detection unit 125c, as shown in Figure 2.

[0027] The colour difference signal calculation unit 125a digitizes the colour difference signal level of a digital video signal input from the switching unit 120 by using Equation (1) below.

$$f(Cb,Cr)=\begin{pmatrix}0, if\left(Cb_L \prec Cb \prec Cb_H\right)\mid\left(Cr_L \prec Cr \prec Cr_H\right)\\ 255, otherwise\end{pmatrix} \quad (1)$$

[0028] Referring to Equation (1), '$Cb_L < Cb < Cb_H$' and '$Cr_L < Cr < Cr_H$' is a predetermined reference colour difference signal level range associated with a particular skin colour. In Equation (1), Cb and Cr denote colour difference signal levels of digital video signals input from the switching unit 120, Cb_L and Cr_L are minimum values of the reference colour difference signal level, and Cb_H and Cr_H are maximum values of the reference colour difference signal level, respectively.

[0029] The colour difference signal calculation unit 125a compares the colour difference signal level of the digital video signal input frame by frame, (i.e. Cb and Cr) with the reference colour difference signal level range predetermined for the particular skin colour decision (i.e. Cb_L, Cr_L ,Cb_H and Cr_H), and digitizes the video signal based upon the results.

[0030] Specifically, the colour difference signal calculation unit 125a digitizes the digital video signal from the switching unit 120 to a colour difference signal level of '0' when the colour difference signal level of the digital video signal is within the predetermined reference colour difference signal level range as in Equation (1), and digitizes the digital video signal to a colour difference signal level of '255' when the colour difference signal level of the digital video signal is excluded from the predetermined reference colour difference level range.

[0031] The filter 125b then filters the digitized digital video signal to remove noise included in the digitized digital video signal.

[0032] The skin colour candidate area detection unit 125c then performs vertical and horizontal projections for the filtered digital video signal to detect at least one skin colour candidate area.

[0033] For example, the vertical projection is used to count the number of pixels, that is, the number of consecutively displayed pixels expressed in the colour difference signal level of '0' in the vertical direction of the filtered digital video signal, and decide if the number of counted pixels is more than a predetermined first threshold value for a skin colour area. Likewise, the horizontal projection is used to count the number of pixels, that is, the number of consecutively displayed pixels expressed in the colour difference signal level of '0' in the horizontal direction of the filtered video signal, and decide if the number of counted pixels is more than a predetermined second threshold value for a skin colour candidate area.

[0034] By doing so, at least one skin colour candidate area having a different size can be detected from the digitized digital video signal of frame unit.

[0035] Returning to Figure 1, the candidate area decision unit 130 normalizes the different sizes of the skin colour candidate areas detected from the skin colour candidate area detection unit 125c to a predetermined size. For example, the candidate area decision unit 130 can normalize all the detected skin colour candidate areas to have a (20×20) pixel resolution.

[0036] Once the size of each skin colour candidate area is normalized, the candidate area decision unit 130 can decide whether each normalized skin colour candidate area is an image for either a human or non-human (i.e. surroundings) image. This decision can be performed by using, for example, the Mahalanobis Distance (MD) method. A detailed description of the MD method is not included as this is well known to those skilled in the art.

[0037] The candidate area storage unit 140 then stores position coordinate values of the skin colour candidate area determined to be a human image, as well as storing the digital video signal for the skin colour candidate area normalized to the predetermined size by the candidate area decision unit 130.

[0038] The control unit 135 controls the overall operations of the monitoring system 100 according to control programs, such as those stored in a program storage unit (not shown) coupled with the control unit.

[0039] The control unit 135 processes the position coordinate values of the skin colour candidate area and the digital video signal for the skin colour candidate area normalized to the predetermined size provided by the candidate area decision unit 130 that is stored in the candidate area storage unit 140.

[0040] Based upon these processes, specifically the detection of a human image, the control unit 135 outputs to the P/T/Z drive unit 110 a zooming control signal for capturing enlarged images of only the skin colour candidate area determined to be a human image by the candidate area decision unit 130, and also outputs a position control signal corresponding to the position coordinate values by reading the position coordinate values of the skin colour candidate area from the candidate area storage unit 140.

[0041] Thus, the image capture unit 105 adaptively traces the skin colour candidate area and captures an enlarged image of the area. Described in more detail, the P/T/Z drive unit 110 moves the image capture unit 105 to a position

where it can capture images of the candidate area based on the position control signal output from the control unit 135, and drives the zoom lens of the image capture unit 105 to zoom in over a predetermined magnification factor to capture an enlarged image of the skin colour candidate area based on the zooming control signal.

[0042] It takes a certain period of time however, for the control unit 135 to output the zooming control signal corresponding to the determined skin colour candidate area. Accordingly, if a particular skin colour candidate area is detected by the candidate area decision unit 130, the control unit 135 outputs a zooming control signal for establishing initial enlargements (i.e. an initial zooming control signal), resulting in a reduction of the response time required for the zooming operation of the image capture unit 105 when the zooming control signal corresponding to the particular skin colour candidate area is provided.

[0043] The initial zooming control signal for establishing initial enlargements is a site-specific signal established to rapidly capture enlarged images, generally targeting an area over a certain size anticipated to include, or be very close to including the determined skin colour candidate area and which can also be stored in the program storage unit. Accordingly, each skin colour candidate area captured in an enlarged image by the initial zooming control signal can be different in size, but is still captured in an enlarged image that can be recognized by a user. That is; by setting up an initial zooming control signal depending on the location and the monitoring areas where the image capture unit 105 is installed, the skin colour candidate area detected in the monitoring areas can be more rapidly captured in an enlarged image in a recognizable size.

[0044] Further, in examples in which one image capture unit 105 sequentially captures images of at least two monitoring areas, a different or an identical initial zooming control signal can be set up for enlarged images of each monitoring area.

[0045] Once a zooming control signal is provided and an enlarged image captured, the analog video signal for a particular skin colour candidate area captured in an enlarged image by the image capture unit 105 is converted into a digital video output signal by ADC 115.

[0046] The switching unit 120 then selectively provides the digital video signal output of the enlarged image from the ADC 115 to the face detection unit 145 based on the controls of the control unit 135.

[0047] The face detection unit 145 is then used to detect a face video signal from the enlarged image digital video signal output.

[0048] Specifically, the face detection unit 145 has a first face candidate area detection unit 145a, a second face candidate area detection unit 145b, and a final face detection unit 145c, as shown in Figure 3.

[0049] The first face candidate area detection unit 145a applies a specific pattern to the enlarged image digital video signal converted by the ADC 115 and detects a face candidate area at which a face probably exists. In an example where an M-grid Gabor Wavelet is applied as the specific pattern, the first face candidate area detection unit 145a matches an '"M"-like shape grid' with a normalized face image, then extracts (20 $\times$ 40) responses as feature vectors. These (20 x 40) responses are obtained from a convolution of 40 (5 frequency $\times$ 8 orientation) Gabor filters at 20 feature points on the grid. The detection unit 145a then performs a learning procedure for calculating a maximum distance with respect to an average of 5 frequency groups in a feature vector space.

[0050] When an enlarged image digital video signal of a unit frame is input, the first face candidate area detection unit 145a matches the '"M"-like shape grid' with all possible positions, extracts feature vectors and performs a detection procedure for calculating a distance with respect to an average vector of the learned 5 frequency groups, respectively. If the minimum distance resulting from the distances calculated in the detection procedure with respect to the average vector is smaller than the maximum distance obtained in the learning procedure, the first face candidate area detection unit 145a decides that the area including feature vectors with the minimum distance is a face candidate area.

[0051] The second face candidate area detection unit 145b uses a low-resolution support vector machine (SVM) to detect a specific candidate area including a specific portion of the face from the detected face candidate area.

[0052] Described in detail, the second face candidate area detection unit 145b performs a Principal Component Analysis (PCA) over a plurality of normalized face images, for example having (20 x 20) resolution in the learning procedure and uses 20 Eigen vectors to extract feature vectors in ascending order of Eigen values. Further, the second face candidate area detection unit 145b uses the above 20 Eigen vectors to extract the feature vectors from randomly collected normalized non-face images, for example as above, having (20 x 20) resolution. Once a plurality of face feature vectors and non-face feature vectors are extracted, the second face candidate area detection unit 145b applies the extracted feature vectors to the SVM to acquire decision boundaries by which two classes, that is, face and non-face images, can be distinguished.

[0053] The second face candidate area detection unit 145b also performs a detection step for detecting a specific candidate area of a face by checking whether the face is included in the respective observation windows in use by the decision boundaries acquired with respect to all possible observation windows of the face candidate area detected from the first face candidate area detection unit 145a.

[0054] The final face detection unit 145c then uses a high-resolution SVM about the detected specific candidate area to finally detect the face. In particular, the final face detection unit 145c detects a face using a method similar to the

decision boundary acquisition and specific candidate area detection of the feature candidate area detection unit 125 as described above.

[0055] However, the final face detection unit 145c uses an image having a (40 x 40) pixel resolution in the learning procedure and uses 50 Eigen vectors to extract features. Further, the final face detection unit 145c then uses the high-resolution SVM about the specific candidate area, including a specific portion of the face detected from the second face candidate area detection unit 125, to finally detect the face.

[0056] A storage and retrieval unit 100a comprises the compression unit 150, the DB generation unit 155, the recording unit 160, the decompression unit 165, the DAC 170 and monitor.

[0057] The compression unit 150, based on the control of the control unit 135 connected via a bus 180, then compresses the digital video signal of each frame unit output from the candidate area detection unit 125 and a face video signal detected from the final face detection unit 145c into a predetermined compression format such as MPEG-2.

[0058] The DB generation unit 155, also based on the control of the control unit 135 connected via the bus 180, then generates a DB for the images of at least one of the digital video signals provided from the compression unit 150, an identification number of the image capture unit 105 producing the digital video signals, and an image-capture time for the video signals.

[0059] Further, the DB generation unit 155 generates a DB for face video signals of the compressed face video signals provided from the compression unit 150 and at least one of an identification number and an enlarged image-capturing time of the image capture unit 105 producing the compressed face video signals.

[0060] The DB for the images produced, and the DB for the face video signals are both recorded on the recording unit 160 under the control of the control unit 135.

[0061] For the recording unit 160, the embodiment of the present invention shown in Figure 1 uses a recording medium such as a hard disc drive (HDD) enabling the mass storage of records.

[0062] The decompression unit 165, based on the control of the control unit 135 connected via the bus 180, can decompress the compressed digital video signal recorded in the recording unit 160 into a predetermined format for providing an output when required.

[0063] The DAC 170 converts the digital video signal decompressed by the decompression unit 165 into an analog video signal. The converted analog video signal is then displayed on a monitor (not shown).

[0064] For use with the units described above, a key manipulation unit 175 is provided, which has a plurality of manipulation keys (not shown) for providing a signal output to the control unit for setting up or manipulating a function supported by the monitoring system 100. The key manipulation unit 175 is connected to the monitoring system 100 through a communication interface unit (not shown) which may be provided in the main body of the monitoring system 100.

[0065] In the embodiment of the present invention shown in Figure 1, the example key manipulation unit 175 has a face recording key 175a for detecting and recording only human face images from a monitoring area taken through the image capture unit 105, and a face searching key 175b for searching for only face video signals from diverse video signals recorded on the recording unit 160.

[0066] For example, if the face recording key 175a is selected, the control unit 135 processes the capturing of enlarged images of human face images from a monitoring area and the recording of the enlarged human face images on the recording unit 160 as described above.

[0067] If the face searching key 175b is selected, the control unit 135 searches for face video signals only from the recording unit 160 and provides the searched face video signals as outputs to the decompression unit 165. Search conditions such as identification numbers, image-capturing times, and so forth, can be applied for rapid and smooth searches.

[0068] In particular, if a certain face video signal is selected by a key manipulation of the key manipulation unit 175 after the face searching key 175b is selected and a plurality of face video signals are reproduced on a monitor, the control unit 135 can control the recording unit 160 and the decompression unit 165 to reproduce all the digital video signals taken at a specific time, such as the same time as the time at which the selected face video signal was taken, or all digital video signals taken by the same image capture unit 105 which also captured the selected face video signal.

[0069] If a certain face video signal is selected by the key manipulation unit 175 and the key manipulation unit 175 outputs a command signal for reproducing entire digital video signals taken at the same time as the selected face video signal was taken (i.e. unenlarged wide-view images taken at the time during which the selected face video signal was detected as described above), the control unit 135 can read-out from the recording unit 160 information on the time at which the selected face video signal was taken (i.e. a read-out time). Further, the control unit 135 can control the recording unit 160 to output entire digital video signals taken at the same time as the read-out time. The control unit 135 can then control the decompression unit 165 to decompress entire digital video signals from the recording unit 160. Thus, a monitor can display entire digital video signals taken during the time when the selected face video signal was taken, so that a user can conveniently search for related surrounding situations in the unenlarged, wide-view images.

[0070] A backup unit (not shown) can also be provided in the monitoring system 100 according to an embodiment of the present invention, which enables digital video signals recorded in the recording unit 160 to be stored as backup data. A recording medium such as a digital audio tape, compact disk, and so on, may be used for the backup unit.

[0071] Figure 4 is a flow chart illustrating an example of a face image detection method for the monitoring system of Figure 1.

[0072] Referring to Figures 1 through Figure 4, at a first step after starting, the ADC 115 converts a video signal taken at a predetermined magnification factor through the image capture unit 105 into a digital video signal (step S400).

[0073] If the digital video signal is provided to the candidate area detection unit 125 by the switching unit 120, the candidate area detection unit 125 compares a colour difference signal level of the converted digital video signal with a predetermined reference colour difference signal level range associated with a particular skin colour and decides whether at least one skin colour candidate area exists, and, if such a skin colour candidate area exists, detects at least one skin colour candidate area (step S410).

[0074] If skin colour candidate areas are detected at step S410, the candidate area decision unit 130 normalizes each detected skin colour candidate area at a predetermined pixel resolution (step S420) and decides whether each normalized skin colour candidate area is a human or non-human (i.e. surroundings) image (step S430). The candidate area storage unit 140 then stores the position coordinate values and video signals for the normalized skin colour candidate areas.

[0075] If it is decided at step S430 that a particular skin colour candidate area is a human image, the image capture unit 105 moves to a position where it can capture images of the skin colour candidate area based on the controls of the P/T/Z drive unit 110 and captures enlarged images of the skin colour candidate area, and the ADC 115 then converts the video signal for enlarged images into an enlarged image digital video signal (step S440).

[0076] The switching unit 120 then provides the enlarged image digital video signal, also referred to as the enlargement digital video signal, to the face detection unit 145.

[0077] The face detection unit 145 decides whether a face video signal exists based on the converted enlarged image digital video signal, and, if decided to exist, detects the face video signal (step S450).

[0078] If the face video signal is detected, the compression unit 150 compresses the detected video signal into a predetermined format (step S460).

[0079] If a face image is detected at step S450, the DB generation unit 155 generates a DB of the compressed face video signal and at least one of the identification number and image-capturing time of the image capture unit 105 which captured the compressed face video signal, and the generated DB is recorded in the recording unit 160 (step S470).

[0080] If a skin colour candidate area is not detected at the step S410, the compression unit 150 compresses the digital video signal of the frame unit which is converted at step S400 into a predetermined format, and the recording unit 160 databases the compressed digital video signal of the frame unit for records (step S480).

[0081] In the monitoring system 100 and the face image detection method according to the embodiment of the present invention as described above, the face image detection can be carried out through various known methods such as face detection based on facial shape information, feature points of a face, pattern-based approach face detection, colour information, and so forth, in addition to the face detection based on the SVM presented in Figure 3.

[0082] As described above, the monitoring system and method is capable of detecting face images. If the monitoring system detects a subject while photographing images of a monitoring area, the system can detect, enlarge and record a subject's face image so that a user can easily search for the subject's face when searching stored image data. Further, the present invention generates a database when recording subject images, so that a user can efficiently search for desired image signals from a large volume of recorded video signals.

[0083] It will be understood that colour difference signal level ranges corresponding to different skin colours can be determined in advance for use as reference colour difference signal level ranges.

[0084] Although the preferred embodiments of the present invention have been described, it will be understood by those skilled in the art that the present invention is not limited to the described preferred embodiments, but various changes and modifications can be made within the scope of the present invention as defined by the appended claims.

Claims

1. An image detection system (100) comprising:

   an image capture unit (105) for capturing an image; **characterised by**
   means (125) for detecting a skin colour candidate area within the image; and
   means (130, 135, 110) responsive to detection of the skin colour candidate area to cause the image capture unit (105) to capture an enlarged image of the skin colour candidate area.

2. An image detection system according to claim 1, further comprising means (145) for detecting a face image from the enlarged image.

3. An image detection system according to claim 1 or 2, wherein the system is arranged to provide a digital video signal representing the image.

4. An image detection system according to claim 3, wherein the skin colour candidate area detecting means (125) further comprises
means (125a) for comparing a colour difference signal level of the digital video signal with a reference range and for digitising the colour difference signal level in dependence on the outcome of the comparison.

5. An image detection system according to claim 4, further comprising means (125c) for detecting a skin colour candidate area based on the digitised colour difference signal level.

6. An image detection system according to claim 5, wherein the digitised colour difference signal level comprises a first level to indicate that the colour difference signal level is within the reference range and a second level to indicate that the colour difference signal level is outside the reference range.

7. An image detection system according to claim 6, wherein the detecting means (125c) is arranged to determine whether the number of displayed pixels having a digitised colour difference signal level at the first level exceed a predetermined threshold.

8. A method of image detection, comprising:

capturing an image using an image capture unit (105); **characterised by**
detecting a skin colour candidate area within the image; and
in response to detection of the skin colour candidate area, causing the image capture unit (105) to capture an enlarged image of the skin colour candidate area.

9. A monitoring system to detect and record an image at a monitored position, the system comprising:

an image-capturing photographing unit adapted to capture at least one photographic image and communicate said image as an image video signal;
a candidate area detection and decision unit adapted to evaluate said image video signal to detect a human skin colour candidate area within said image and if detected, to direct said image-capturing photographing unit to capture at least one enlarged photographic image of said human skin colour candidate area and output said enlarged photographic image as an enlarged image video signal;
a face detection unit adapted to evaluate said enlarged image video signal to detect a face video signal within said enlarged image video signal; and
a storage and retrieval unit to receive and store said detected face video signal.

10. A monitoring system to detect and record an image at a monitored position as claimed in claim 9, wherein said candidate area detection and decision unit further comprising:

a colour difference signal calculation unit adapted to compare a colour difference signal level of said video signal with a reference range and to digitize said video signal as a first or second value based upon said comparison; and
a skin colour candidate area detection unit adapted to compare at least one of said first and second values with a threshold value detect a skin colour candidate area.

11. A monitoring system to detect and record an image at a monitored position as claimed in claim 10, wherein:

said first value indicates a colour difference signal level of said video signal within said reference range; and
said second value indicates a colour difference signal level of said video signal outside said reference range.

12. A monitoring system to detect and record an image at a monitored position as claimed in claim 10, wherein said candidate area detection and decision unit further comprises:

a decision unit adapted to normalize said skin colour candidate area and to determine if said normalized skin colour candidate area is a human skin colour candidate area.

13. A monitoring system to detect and record an image at a monitored position as claimed in claim 9, wherein said face detection unit further comprises:

a first face candidate area detection unit adapted to use a pattern with said enlarged image video signal to detect a face candidate area;
a second face candidate area detection unit adapted to use a low-resolution support vector machine to detect a specific candidate area within said detected face candidate area; and
a final face detection unit adapted to use a high-resolution support vector machine to detect a face video signal within said specific candidate area.

14. A monitoring system to detect and record an image at a monitored position as claimed in claim 13, wherein:

said first face candidate area detection unit uses an M-Grid Gabor Wavelet pattern with said enlarged image video signal to detect said face candidate area.

15. A monitoring system to detect and record an image at a monitored position as claimed in claim 13, wherein:

said second face candidate area detection unit uses a Principal Component Analysis to generate a plurality of face and non-face feature vectors for use with said support vector machine.

16. A monitoring system to detect and record an image at a monitored position as claimed in claim 9, wherein said storage and retrieval unit further comprises:

a compression/decompression unit to compress or decompress at least one of said image video signal, enlarged image video signal and detected face video signal;
a data base generation unit to create a data base based upon at least one of said image video signal, enlarged image video signal and detected face video signal;
a recording unit to store at least one of said image video signal, enlarged image video signal and detected face video signal; and
a monitor to display at least one of said image video signal, enlarged image video signal and detected face video signal.

17. A monitoring system for detecting and recording an image at a monitored position as claimed in claim 9, wherein said storage and retrieval unit further comprises:

a key manipulation unit to direct said capturing, storage and retrieval of at least one of said image video signal, enlarged image video signal and detected face video signal.

18. A monitoring system to detect and record an image at a monitored position as claimed in claim 9, wherein:

said photographing unit further comprises a pan, tilt and zoom mechanism for capturing said photographic image and said enlarged photographic image.

19. A monitoring system to detect and record an image at a monitored position as claimed in claim 9, further comprising a switching unit adapted to selectively switch one among said candidate area detection and decision unit and said face detection unit to provide said image video signal.

20. A monitoring system to detect and record an image at a monitored position as claimed in claim 10, further comprising a filter adapted to filter noise from said digitized video signal.

21. A monitoring system for analysis, storage and retrieval of an image, the system comprising:

an image photographing unit adapted to capture at least one of a normal and an enlarged video signal of an image;
a candidate detection unit adapted to evaluate said captured normal video signal to detect a human skin

candidate area based upon a colour range and control said image photographing unit to capture an enlarged video signal of said human skin candidate area;
a face detection unit adapted to evaluate said captured enlarged video signal of said human skin candidate area to detect a face image video signal; and
a storage and retrieval unit adapted to store said face image video signal.

22. A monitoring system for analysis, storage and retrieval of an image as claimed in claim 21, further comprising:

a data base of said face image video signals adapted to allow a user to search for a desired normal, enlarged and face image video signal from a large amount of recorded video signals.

23. A method to detect and record an image at a monitored position, the method comprising the steps of:

converting an analog image video signal taken at a predetermined magnification factor through an image capturing unit into a digital image video signal and evaluating said digital image video signal to determine if a human skin colour candidate area is detected, and if said candidate area is detected, controlling said image capturing unit to capture an enlarged analog image video signal of said human skin colour candidate area; and converting said enlarged analog image video signal into an enlarged digital image video signal and evaluating said enlarged digital signal to determine if a face image video signal is detected, and if said face image video signal is detected, recording said face image video signal.

24. A method to detect and record an image at a monitored position as claimed in claim 23, further comprising the step of:

comparing a colour difference signal level of said digital image video signal with a colour reference range to determine if said human skin colour candidate area is detected; and
applying al least one of a pattern, low-resolution support vector machine and a high-resolution support vector machine to detect said face image video signal.

25. A method to detect and record an image at a monitored position as claimed in claim 23, wherein said recording said face image video signal further comprises the steps of:

compressing said face image video signal and generating a face image data base for said signal; and
recording said compressed face image video signal and said data base.

FIG. 1

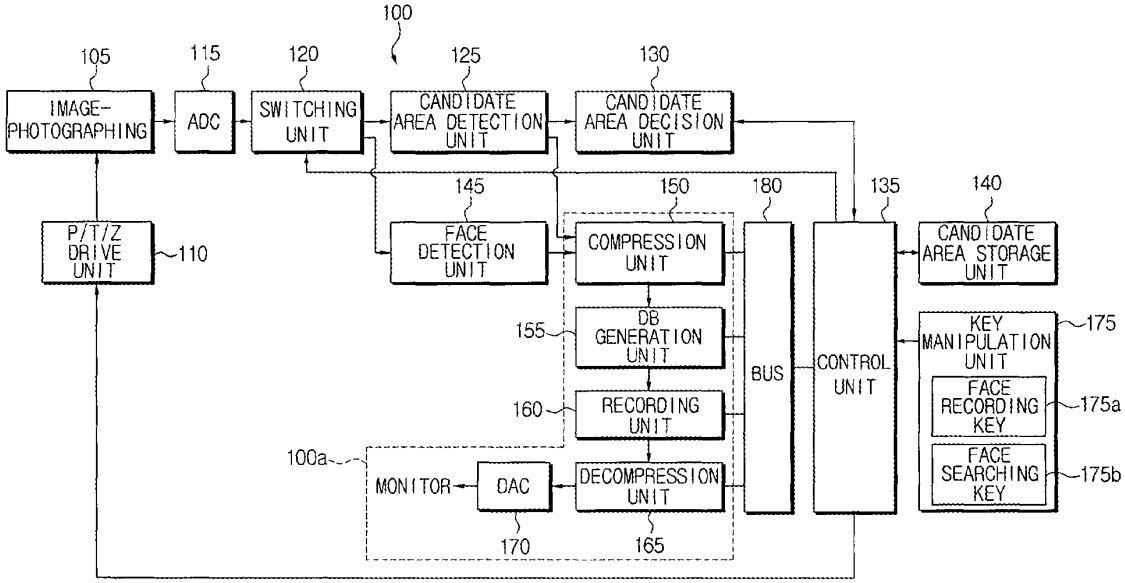

100
105
IMAGE-PHOTOGRAPHING
115
ADC
120
SWITCHING UNIT
125
CANDIDATE AREA DETECTION UNIT
130
CANDIDATE AREA DECISION UNIT
145
FACE DETECTION UNIT
150
COMPRESSION UNIT
180
BUS
135
CONTROL UNIT
140
CANDIDATE AREA STORAGE UNIT
P/T/Z DRIVE UNIT
110
155
DB GENERATION UNIT
160
RECORDING UNIT
KEY MANIPULATION UNIT
175
FACE RECORDING KEY
175a
FACE SEARCHING KEY
175b
100a
MONITOR
DAC
170
DECOMPRESSION UNIT
165

FIG. 2

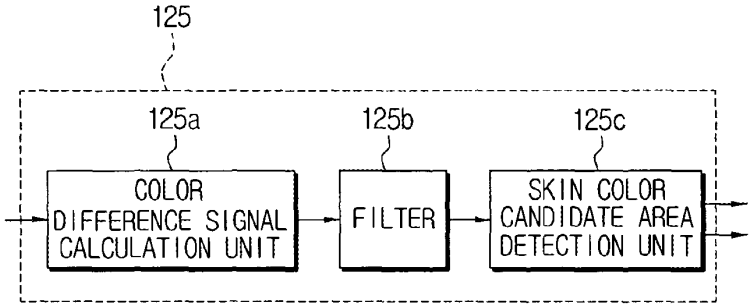

125
125a
125b
125c
COLOR DIFFERENCE SIGNAL CALCULATION UNIT
FILTER
SKIN COLOR CANDIDATE AREA DETECTION UNIT

FIG. 3

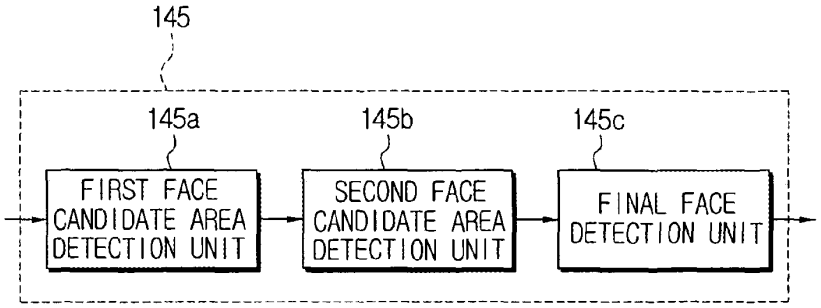
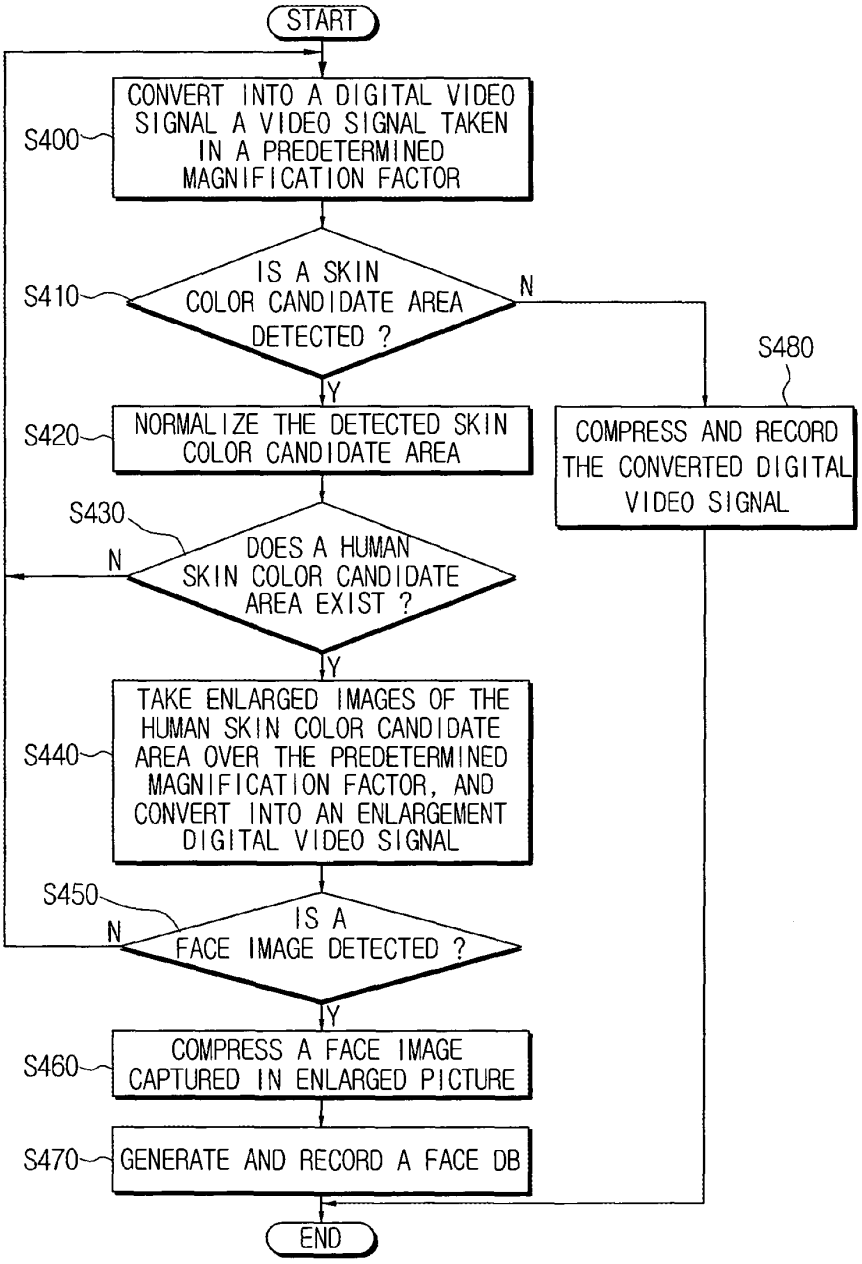

145
145a
145b
145c
FIRST FACE CANDIDATE AREA DETECTION UNIT
SECOND FACE CANDIDATE AREA DETECTION UNIT
FINAL FACE DETECTION UNIT

FIG. 4


START
S400
CONVERT INTO A DIGITAL VIDEO SIGNAL A VIDEO SIGNAL TAKEN IN A PREDETERMINED MAGNIFICATION FACTOR
S410
IS A SKIN COLOR CANDIDATE AREA DETECTED ?
N
Y
S480
COMPRESS AND RECORD THE CONVERTED DIGITAL VIDEO SIGNAL
S420
NORMALIZE THE DETECTED SKIN COLOR CANDIDATE AREA
S430
DOES A HUMAN SKIN COLOR CANDIDATE AREA EXIST ?
N
Y
S440
TAKE ENLARGED IMAGES OF THE HUMAN SKIN COLOR CANDIDATE AREA OVER THE PREDETERMINED MAGNIFICATION FACTOR, AND CONVERT INTO AN ENLARGEMENT DIGITAL VIDEO SIGNAL
S450
IS A FACE IMAGE DETECTED ?
N
Y
S460
COMPRESS A FACE IMAGE CAPTURED IN ENLARGED PICTURE
S470
GENERATE AND RECORD A FACE DB
END

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 04 25 1267

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	HONGO H ET AL: "Face and hand gesture recognition for human-computer interaction" PATTERN RECOGNITION, 2000. PROCEEDINGS. 15TH INTERNATIONAL CONFERENCE ON SEPTEMBER 3-7, 2000, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 3 September 2000 (2000-09-03), pages 921-924, XP010533963 ISBN: 0-7695-0750-6	1-6,8	G06K9/00 G06K9/62
Y	* the whole document *	7,9-13, 15-25	

Y	ACOSTA E ET AL: "An automatic face detection and recognition system for video indexing applications" 2002 IEEE INTERNATIONAL CONFERENCE ON ACOUSTICS, SPEECH, AND SIGNAL PROCESSING. PROCEEDINGS (CAT. NO.02CH37334), PROCEEDINGS OF INTERNATIONAL CONFERENCE ON ACOUSTICS, SPEECH AND SIGNAL PROCESSING (CASSP'02), ORLANDO, FL, USA, 13-17 MAY 2002, pages IV3644-IV3647 vol.4, XP002281463 2002, Piscataway, NJ, USA, IEEE, USA ISBN: 0-7803-7402-9 * the whole document *	7,9-12, 16-22	TECHNICAL FIELDS SEARCHED (Int.Cl.7) G06K

Y	ALBIOL A ET AL: "A simple and efficient face detection algorithm for video database applications" IMAGE PROCESSING, PROC. OF 7TH INT. IEEE CONF., vol. 2, 10 September 2000 (2000-09-10), pages 239-242, XP010529968 * the whole document *	7,9-12, 16-22	

	-/--		

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
MUNICH	25 May 2004	Müller, M

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 04 25 1267

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
Y A	US 2002/190119 A1 (HUFFMAN JOHN W) 19 December 2002 (2002-12-19) * abstract; figures 1-5 * * paragraph [0001] - paragraph [0009] *	23-25 9,21	
Y A	EP 1 260 934 A (MATSUSHITA ELECTRIC IND CO LTD) 27 November 2002 (2002-11-27) * paragraph [0001] - paragraph [0033] * * paragraph [0039] - paragraph [0047]; claim 11 *	23-25 9,16,21	
A	KRUGER V ET AL: "Gabor wavelet networks for efficient head pose estimation" BMVC2000. PROCEEDINGS OF THE 11TH BRITISH MACHINE VISION CONFERENCE, BRISTOL, UK, 11-14 SEPT. 2000, vol. 20, no. 9-10, pages 665-672, XP002281464 Image and Vision Computing, 1 Aug. 2002, Elsevier, Netherlands ISSN: 0262-8856 * the whole document *	24	TECHNICAL FIELDS SEARCHED (Int.Cl.7)

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
MUNICH	25 May 2004	Müller, M

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 04 25 1267

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	ZHENGYOU ZHANG ET AL: "Comparison between geometry-based and Gabor-wavelets-based facial expression recognition using multi-layer perceptron" PROCEEDINGS THIRD IEEE INTERNATIONAL CONFERENCE ON AUTOMATIC FACE AND GESTURE RECOGNITION (CAT. NO.98EX107), PROCEEDINGS THIRD IEEE INTERNATIONAL CONFERENCE ON AUTOMATIC FACE AND GESTURE RECOGNITION, NARA, JAPAN, 14-16 APRIL 1998, pages 454-459, XP002281465 1998, Los Alamitos, CA, USA, IEEE Comput. Soc, USA ISBN: 0-8186-8344-9 * abstract; figure 3 * * page 454 - page 456, left-hand column, paragraph 1 * ---	24	
Y	GARCIA C ET AL: "Face detection in color images using wavelet packet analysis" MULTIMEDIA COMPUTING AND SYSTEMS, 1999. IEEE INTERNATIONAL CONFERENCE ON FLORENCE, ITALY 7-11 JUNE 1999, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 7 June 1999 (1999-06-07), pages 703-708, XP010342795 ISBN: 0-7695-0253-9 * the whole document * --- -/--	13,15	TECHNICAL FIELDS SEARCHED (Int.Cl.7)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
MUNICH	25 May 2004	Müller, M

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 04 25 1267

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
P,A	BYUN H ET AL: "ROBUST FACE DETECTION AND TRACKING FOR REAL-LIFE APPLICATIONS" INTERNATIONAL JOURNAL OF PATTERN RECOGNITION AND ARTIFICIAL INTELLIGENCE, WORLD SCIENTIFIC PUBLISHING COMPAGNY, SINGAPORE, SI, vol. 17, no. 6, September 2003 (2003-09), pages 1035-1055, XP001171782 ISSN: 0218-0014 * page 1039, paragraph 3 - page 1047, paragraph 1 * -----	24	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
MUNICH	25 May 2004	Müller, M

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 04 25 1267

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

25-05-2004

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002190119 A1	19-12-2002	NONE	
EP 1260934 A	27-11-2002	EP 1260934 A2	27-11-2002
		JP 2003046911 A	14-02-2003
		US 2002175997 A1	28-11-2002

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

Espacenet

Bibliographic data: WO2006130542 (A1) — 2006-12-07

USING PHOTOGRAPHER IDENTITY TO CLASSIFY IMAGES

Inventor(s): GALLAGHER ANDREW CHARLES [US]; WELDY JOHN ALLAN [US] ± (GALLAGHER, ANDREW CHARLES, ; WELDY, JOHN ALLAN)

Applicant(s): EASTMAN KODAK CO [US]; GALLAGHER ANDREW CHARLES [US]; WELDY JOHN ALLAN [US] ± (EASTMAN KODAK COMPANY, ; GALLAGHER, ANDREW CHARLES, ; WELDY, JOHN ALLAN)

Classification: **- international:** ***G06F17/30; G06K9/00***
- cooperative: **G06K9/00288**; **G06K9/00697**

Application number: WO2006US20712 20060530

Priority number (s): US20050143541 20050602

Also published as: US2009046933 (A1) US7574054 (B2) US2006274949 (A1) JP2008543224 (A) JP4908505 (B2) more

Abstract of WO2006130542 (A1)

A method of identifying at least one particular person of interest in a collection of digital images taken over time, includes providing the collection of digital images with each digital image containing one or more persons; storing in a digital database an appearance model having a set of features associated with the particular person of interest and a prior probability of the person of interest appearing in images by a particular photographer; and comparing the appearance model with features extracted from the digital images in the collection of digital images and using the prior probability and the appearance model to determine if the particular person of interest is in one or more digital images in the collection of digital images.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 December 2006 (07.12.2006)

PCT

(10) International Publication Number
WO 2006/130542 A1

(51) International Patent Classification:
G06K 9/00 (2006.01) *G06F 17/30* (2006.01)

(21) International Application Number:
PCT/US2006/020712

(22) International Filing Date: 30 May 2006 (30.05.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/143,541 2 June 2005 (02.06.2005) US

(71) Applicant *(for all designated States except US)*: **EASTMAN KODAK COMPANY** [US/US]; 343 State Street, Rochester, New York 14650-2201 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **GALLAGHER, Andrew Charles** [US/US]; 353 Campbell Road, Rochester, New York 14420 (US). **WELDY, John Allan** [US/US]; 2326 St. Paul Street, Rochester, New York 14621 (US).

(74) Common Representative: **EASTMAN KODAK COMPANY**; 343 State Street, Rochester, New York 14650-2201 (US).

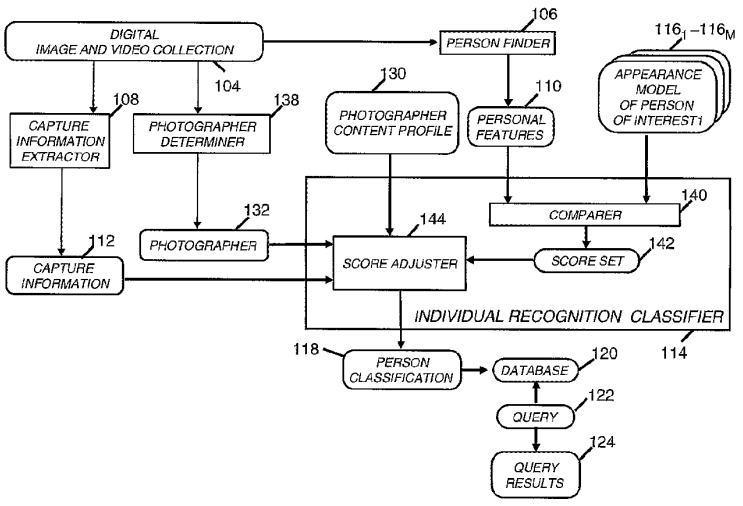
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: USING PHOTOGRAPHER IDENTITY TO CLASSIFY IMAGES



(57) Abstract: A method of identifying at least one particular person of interest in a collection of digital images taken over time, includes providing the collection of digital images with each digital image containing one or more persons; storing in a digital database an appearance model having a set of features associated with the particular person of interest and a prior probability of the person of interest appearing in images by a particular photographer; and comparing the appearance model with features extracted from the digital images in the collection of digital images and using the prior probability and the appearance model to determine if the particular person of interest is in one or more digital images in the collection of digital images.

WO 2006/130542 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

USING PHOTOGRAPHER IDENTITY TO CLASSIFY IMAGES

FIELD OF THE INVENTION

The invention relates to image processing and more particularly relates to the identification or recognition of a person of interest in a collection of digital images or videos.

BACKGROUND OF THE INVENTION

With the advent of digital photography, consumers are amassing large collections of digital images and videos. The average number of images captures with digital cameras per photographer is still increasing each year. As a consequence, the organization and retrieval of images and videos is already a problem for the typical consumer. Currently, the length of time spanned by a typical consumer's digital image collection is only a few years. The organization and retrieval problem and its complexity will continue to grow as the length of time spanned by the average digital image and video collection increases and the sources for image content also increases.

Descriptors of a photographer, such as biometric data, can be detected and/or recorded in an image capture device such as a digital camera.

US Patent Application Publication US 2003/235411A1 discloses an imaging apparatus wherein a biological recording means records biological information of a photographer and subsequently uses this information to control the imaging apparatus.

U.S. Patent No. 6,433,818 describes a camera with built-in apparatus for acquiring measured biometric data of a potential user, comparing it with corresponding biometric signature data entered in the camera, and allowing camera operation only if there is a match. This function provides security and prevents unauthorized access to the data stored on the camera, thereby discouraging theft.

U.S. Patent Application Publication US 2002/0080256A1 describes a digital camera with built-in apparatus for biometric identification of the photographer and for recording the identification of the photographer of an image. Furthermore, this feature can be used to discourage theft or piracy of the camera.

Preferably, an image of the photographer's iris is captured to determine the identity of the photographer.

One of the most prevalent image content subjects of photography is people. Furthermore, in a given collection of digital images and videos, certain people tend to occur frequently. For example, it is common for most images captured by new parents to contain their new baby. Consumers desire the ability to find all images from their collection containing a specific person.

SUMMARY OF THE INVENTION

It is an object of the present invention to make use of the fact that a particular photographer has captured the images in a collection to find objects of interest in the collection.

This object is achieved by a method of identifying at least one particular person of interest in a collection of digital images taken over time, comprising:

providing the collection of digital images with each digital image containing one or more persons;

storing in a digital database an appearance model having a set of features associated with the particular person of interest and a prior probability of the person of interest appearing in images by a particular photographer; and

comparing the appearance model with features extracted from the digital images in the collection of digital images and using the prior probability and the appearance model to determine if the particular person of interest is in one or more digital images in the collection of digital images.

It is an advantage of the present invention that when a known photographer has taken images in a collection, that fact can be used to find images of interest. This is made possible because the likelihood that an object of interest appears in an image is related to the identity of the photographer.

It is a further advantage of the invention that knowledge of the identity of the particular photographer of an image can be used in determining the orientation of the captured image and whether the image was captured indoors or outdoors.

BRIEF DESCRIPTION OF THE DRAWINGS

The above-mentioned and other features and objects of this invention and the manner of attaining them will become more apparent and the invention itself will be better understood by reference to the following description of an embodiment of the invention taken in conjunction with the accompanying figures wherein:

FIG. 1 is a schematic diagram of computer system that can implement the present invention;

FIG. 2 is a flow chart of an embodiment of the present invention;

FIGS. 3A and 3B are appearance models of a person of interest having different associated times;

FIG. 4 is a more detailed flow chart of an embodiment of the present invention;

FIG. 5 is flow chart of an alternative embodiment of the present invention; and

FIGS. 6A-6D illustrate four different image orientations.

DETAILED DESCRIPTION OF THE INVENTION

In the following description, some embodiments of the present invention will be described as software programs and/or algorithmic flow diagrams. Those skilled in the art will readily recognize that the equivalent of such software can also be constructed in hardware. Because image manipulation algorithms and systems are well known, the present description will be directed in particular to algorithms and systems forming part of, or cooperating more directly with, the method in accordance with the present invention. Other aspects of such algorithms and systems, and hardware and/or software for producing and otherwise processing the image signals involved therewith, not specifically shown or described herein can be selected from such systems, algorithms, components, and elements known in the art. Given the description as set forth in the following specification, all software implementation thereof is conventional and within the ordinary skill in such arts.

The present invention can be implemented in computer hardware and computerized equipment. For example, the method can be performed in a digital camera or other digital image capture devices, a digital printer, on an internet server, on a kiosk, and on a personal computer. Referring to FIG. 1, there is illustrated a computer system for implementing the present invention. Although the computer system is shown for the purpose of illustrating a preferred embodiment, the present invention is not limited to the computer system shown, but can be used on any electronic processing system such as found in digital cameras, cell phones, portable computing devices, home computers, kiosks, retail or wholesale photofinishing, or any other system for the processing of digital images. The computer system includes a microprocessor-based unit 20 (also referred to herein as a digital image processor) for receiving and processing software programs and for performing other processing functions. The digital image processor 20 processes images from image capture devices 10 such as cameras, scanners, or computer image generation software. The digital image processor 20 can be used to process digital images to make adjustments for overall brightness, tone scale, image structure, etc. of digital images in a manner such that a pleasing looking image is produced by an image output device. The digital image processor 20 interfaces with the general control computer 40 (also a microprocessor based unit) for exchanging data and commands. The general control computer 40 and the digital image processor 20 can be two different microprocessors, or the functions of each can be performs by a single physical microprocessor. The digital image processor 20 often outputs an image to an image output device 30 for example a printer for displaying the image. A display device 50 is electrically connected to the digital image processor 20 for displaying user-related information associated with the software, e.g., by means of a graphical user interface. A keyboard 60 is also connected to the microprocessor based unit 20 via the general control computer 40 for permitting a user to input information to the software. As an alternative to using the keyboard 60 for input, a mouse can be used for moving a selector on the display device 50 and for selecting an item on which the selector overlays, as is well known in the art.

A compact disk-read only memory (CD-ROM) which typically includes software programs, is inserted into the general control computer 40 for providing a means of inputting the software programs and other information to the general control computer 40 and the digital image processor 20. In addition, a floppy disk can also include a software program, and is inserted into the general control computer 40 for inputting the software program. Still further, the general control computer 40 can be programmed, as is well known in the art, for storing the software program internally. The general control computer 40 can have a network connection, such as a telephone line or wireless connection, to an external network, such as a local area network or the Internet.

Images can also be displayed on the display device 50 via a personal computer card (PC Card), such as, as it was formerly known, a PCMCIA card (based on the specifications of the Personal Computer Memory Card International Association) which contains digitized images electronically embodied in the card.

The image output device 30 provides a final image. The output device 30 can be a printer or other output device that provides a paper or other hard copy final image. The output device 30 can also be an output device that provides the final image as a digital file. The output device 30 can also include combinations of output, such as a printed image and a digital file on a memory unit, such as a CD or DVD. Digital images and other data are stored on an offline memory device 70 such as an external hard drive, flash media, a drive that writes to CD-ROM or DVD media , or the like.

A digital image includes one or more digital image channels or color components. Each digital image channel is a two-dimensional array of pixels. Each pixel value relates to the amount of light received by the imaging capture device corresponding to the physical region of pixel. For color imaging applications, a digital image will often consist of red, green, and blue digital image channels. Motion imaging applications can be thought of as a sequence of digital images. Those skilled in the art will recognize that the present invention can be applied to, but is not limited to, a digital image channel for any of the herein-

mentioned applications. Although a digital image channel is described as a two dimensional array of pixel values arranged by rows and columns, those skilled in the art will recognize that the present invention can be applied to non rectilinear arrays with equal effect. Those skilled in the art will also recognize that for digital image processing steps described hereinbelow as replacing original pixel values with processed pixel values is functionally equivalent to describing the same processing steps as generating a new digital image with the processed pixel values while retaining the original pixel values.

It should also be noted that the present invention can be implemented in a combination of software and/or hardware and is not limited to devices which are physically connected and/or located within the same physical location. One or more of the devices illustrated in FIG. 1 can be located remotely and can be connected via a network. One or more of the devices can be connected wirelessly, such as by a radio-frequency link, either directly or via a network.

The present invention can be employed in a variety of user contexts and environments. Exemplary contexts and environments include, without limitation, wholesale digital photofinishing (which involves exemplary process steps or stages such as film in, digital processing, prints out), retail digital photofinishing (film in, digital processing, prints out), home printing (home scanned film or digital images, digital processing, prints out), desktop software (software that applies algorithms to digital prints to make them better -or even just to change them), digital fulfillment (digital images in - from media or over the web, digital processing, with images out - in digital form on media, digital form over the web, or printed on hard-copy prints), kiosks (digital or scanned input, digital processing, digital or hard copy output), mobile devices (e.g., PDA or cell phone that can be used as a processing unit, a display unit, or a unit to give processing instructions), and as a service offered via the World Wide Web.

In each case, the invention can stand alone or can be a component of a larger system solution. Furthermore, human interfaces, e.g., the scanning or input, the digital processing, the display to a user (if needed), the input of user requests or processing instructions (if needed), the output, can each be on the same

or different devices and physical locations, and communication between the devices and locations can be via public or private network connections, or media based communication. Where consistent with the foregoing disclosure of the present invention, the method of the invention can be fully automatic, can have user input (be fully or partially manual), can have user or operator review to accept/reject the result, or can be assisted by metadata (metadata that can be user supplied, supplied by a measuring device (e.g. in a camera), or determined by an algorithm). Moreover, the algorithm(s) can interface with a variety of workflow user interface schemes.

The invention is inclusive of combinations of the embodiments described herein. References to "a particular embodiment" and the like refer to features that are present in at least one embodiment of the invention. Separate references to "an embodiment" or "particular embodiments" or the like do not necessarily refer to the same embodiment or embodiments; however, such embodiments are not mutually exclusive, unless so indicated or as are readily apparent to one of skill in the art.

A first embodiment of this method is illustrated in FIG. 2. A digital image and video collection 104 is analyzed to recognize the identities of the people therein. Recognition of the people in a collection of the digital images or videos 104 allows for the creation of a database 120 relating digital images or videos 104 and the identities of the people in the digital images or videos 104. Consequently, the database 120 can be queried 122 to find those images and videos containing the query person of interest. The database 120 can be in any form. The database 120 can be distributed across many files, by for example, inserting a person classification 118 into the file header of the digital image or video 104. For example, a query 122 for images of "Jim" returns query results 124 containing the set of digital images or videos 104 containing the person of interest "Jim". Then the query results 124 can be returned. The query results 124 are the set of digital images and videos 104 containing the query person of interest. The digital images and videos 104 of the query result 124 can be displayed on a display device 50 as shown in FIG. 1 for review by the user.

In the system, the digital image or video 104 is passed to the capture information extractor 108. The capture information extractor 108 determines the capture information 112 related to the capture of the digital image and videos 104 of the collection, and outputs the resulting information, where capture information 112 related to a particular digital image or video 104 is associated with that particular digital image or video 104. The capture information 112 can be the time a particular digital image or video 104 was captured, the location the image or video was captured, the focal length, the subject distance, the number of rows and columns of pixels, the magnification, whether the flash was fired, whether the self-timer was activated, etc. The capture information 112 for a particular image or video is determined by one of several methods by the capture information extractor 108. Often times, capture information 112 is embedded in the file header of the digital image or video 104. For example, the EXIF image format (described at www.exif.org) allows the image or video capture device to store information associated with the image or video in the file header. The "Date\Time" entry is associated with the date and time the image was captured. In some cases, the digital image or video results from scanning film and the image capture time is determined by detection of the date printed into the image (as is often done at capture time) area, usually in the lower left corner of the image. The date a photograph is printed is often printed on the back of the print. Alternatively, some film systems contain a magnetic layer in the film for storing information such as the capture date. The capture information extractor 108 uses the most appropriate method for extracting the capture information 112 of the image. Preferably, the source of the digital images and videos is a digital camera, and the capture information extractor 108 extracts the capture information from the image file information.

The images and videos of the collection are also analyzed by the photographer determiner 138 to determine the identity of the particular photographer for each image and video. When the EXIF file format is used, the identity of the photographer can be stored in the "Camera Owner"," Image Creator", "Photographer", or "Copyright" tags for example. The identity of the

photographer of an image or video can be entered manually before, during, or after capturing the video. Furthermore, several cameras (e.g. in U.S. Patent Application Publication US 2002/0080256A1) have been described that contain means for extracting biometric information from the photographer, identifying the photographer, and then annotating the image with the identity of the photographer. In any case, the photographer determiner 138 discovers the identity of the photographer 132 and passes that information to the individual recognition classifier 114. In some cases, the photographer 132 can not be able to be identified by the photographer determiner 138. In this case, the photographer 132 is "unknown". For example, this situation can occur when a person who owns the camera is on vacation and asks a stranger to use her (the vacationing camera owner) camera to capture an image of her in front of a landmark. A camera such as described in U.S. Patent Application US 2002/0080256A1 can only feasibly identify the photographer from a small set of potential camera users (e.g. the primary user is probably the camera owner, and secondary users are friends and family of the camera owner) whose profiles are known by the camera. In this case, an image captured by a stranger using the camera would simply be identified by the photographer determiner 138 as having an "unknown" photographer 132.

Image capture time can be included in the capture information 112 and can be a precise minute in time, e.g. March 27, 2004 at 10:17 AM. Or the image capture time can be less precise, e.g. 2004 or March 2004. The image capture time can be in the form of a probability distribution function e.g. March 27, 2004 +/- 2 days with 95 % confidence. The image capture time is input to the individual recognition classifier 114.

The person finder 106 identifies one or more persons in the digital video or digital image. Preferably, people are found by face detection. Methods for detecting human faces are well known in the art of digital image processing. For example, a face detection method for finding human faces in images is described in the following article: Jones, M.J.; Viola, P., "Fast Multi-view Face Detection", *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2003. Furthermore, once a face is detected, the facial features (e.g.

eyes, nose, mouth, etc.) can also be localized using well known methods such as described by Yuille et al. in, "Feature Extraction from Faces Using Deformable Templates," Int. Journal of Comp. Vis., Vol. 8, Iss. 2, 1992, pp. 99-111. The authors describe a method of using energy minimization with template matching for locating the mouth, eye and iris/sclera boundary. Facial features can also be found using active appearance models as described by T. F. Cootes and C. J. Taylor "Constrained active appearance models", *8th International Conference on Computer Vision*, volume 1, pages 748–754. IEEE Computer Society Press, July 2001.

Alternatively, different facial features can also be used. For example, an embodiment can be based upon the facial similarity metric described by M. Turk and A. Pentland in "Eigenfaces for Recognition" *Journal of Cognitive Neuroscience. Vol 3, No. 1. 71-86, 1991.* Facial descriptors are obtained by projecting the image of a face onto a set of principal component functions that describe the variability of facial appearance. The similarity between any two faces is measured by computing the Euclidean distance of the features obtained by projecting each face onto the same set of functions. In this case, an appearance model can describe the mean and covariance of the projection of multiple images of the same face onto these principal component functions. The similarity metric (for example computed by comparer 140 of FIG. 4) can calculate the Mahalonobis of a new face to the mean of the model.

The appearance model and similarity measurement could include a combination of several disparate feature types such as Eigenfaces, facial measurements, color/texture information, wavelet features etc.

A person finder 106 outputs personal features 110 that are quantitative descriptions of a person detected by the person detector 106. Preferably, the person finder 106 outputs one set of personal features 110 for each detected person. Preferably the personal features are the locations of 82 feature points associated with specific facial features, found using a method similar to the aforementioned active appearance model of Cootes et al. A visual representation of the facial feature points for an image of a face is shown in FIG. 3A and FIG. 3B

as an illustration. Alternatively, the personal features 110 can additionally be represented with quantifiable descriptors such as eye color, skin color, face shape, etc. The personal features 110 can also be distances between specific feature points or angles formed by lines connecting sets of specific feature points. Color cues are easily extracted from the digital image or video 104 once the person and facial features are located by the person finder 106. The personal features 110 are input to the individual recognition classifier 114.

A set of appearance models $116_1 - 116_M$ of M persons of interest from a stored digital database is input to the individual recognition classifier 114 for determining the identity of each of the persons detected by the person finder 106 and represented by the personal features 110. The appearance models $116_1 - 116_M$ contain a set of features associated with a particular person of interest. Each appearance model for an individual of interest can include a number of sub-models, for example models describing the appearance of the person of interest at different ages as described in above-cited co-pending application U.S. Patent Application Serial No. 11/116,729. Or the sub-models could describe the appearance of the person of interest with different appearances (e.g. one sub-model represents the appearance of the person of interest with facial hair, another sub-model represents the appearance of the person of interest without facial hair). The appearance model will be discussed in greater detail hereinbelow. A person of interest is a person that is important to identify in a collection of digital images and videos 104. For example, in a household with small children, each child would likely be a person of interest because it would be useful and valuable for a head of the household to identify occurrences of each child in each photo and video 104 of the digital media collection. The aforementioned camera owner, as primary photographer, can be a person of interest as can be any secondary photographers (i.e. friends and family of the camera owner). The purpose of the individual recognition classifier 114 is to use one or more of the appearance models 116_1–116_M, the image capture information 112, and the personal features 110 to determine if a person detected by the person finder 106 is a particular

person of interest. This is accomplished by comparing the personal features 110 of the detected person with the features of the appearance model 116 of the particular person of interest. The individual recognition classifier 114 outputs the person classification 118. Typically, the individual recognition classifier outputs a high probability that a person detected by the person finder 106 is a particular person of interest *m* when the personal features 110 associated with the detected person are similar to the appearance model 116*m* associated with the particular person of interest *m*. Preferably, the person classification 118 is the likelihood (probability) that the person detected by the person finder 106 is the person of interest. The person classification 118 can be a binary indicator (e.g. true of false) indicating the classifier's decision on whether the person associated with the personal features 110 is the person of interest.

By repeating the application of the individual recognition classifier 114 to each person detected in each digital image or video 104 of a collection, all persons detected by the person finder 106 are classified as to the likelihood that each is the particular person of interest.

The person classification 118 can then be associated with digital image or video containing the detected person. For example, an image can be tagged or annotated in the database 120 as containing the person of interest "Mary". Furthermore, the person classification 118 information can be associated with the personal features 110. Furthermore, the image can also be tagged with the location within the digital image or video of the person detected by the person finder 106 that the individual recognition classifier 114 determined was the person of interest. Furthermore, the likelihood or probability of the person classification 118 can be added to the annotation in the database 120 as well. When the query 122 is made for digital images or videos 104 containing a particular person of interest, the database 120 is searched and the appropriate query results 124 are returned to the user on a user interface such as the display device 50 of FIG. 1.

The individual recognition classifier uses the photographer 132 information as follows: When the image capture information 112 indicates that the camera's self-timer was used to capture a particular image or video, then the

individual recognition classifier 114 outputs the person classification 118 indicating a high likelihood (probability) that the digital image or video 104 contains the photographer 132. For example, the probability is in the range of 0.75 to 1.0, depending on the particular photographer 132. This results from the fact that most times, the camera self-timer is used to allow time for the photographer 132 to activate the camera then run to be included in the scene captured by the camera in the particular digital image or video 104.

Likewise, when the image capture information 112 indicates that the camera's image or video capture was activated via remote control, then the individual recognition classifier 114 outputs a person classification 118 indicating a medium likelihood (probability) that the digital image or video 104 contains the photographer 132. This results from the fact that often times, the camera's image or video capture is activated using remote control to allow time the photographer 132 to be in the scene captured by the camera in the particular digital image or video 104. However, remote activation of the camera's capture sequence can also be used to avoid shaking the camera. For this reason, the probability associated with the person classification 118 indicating that the photographer 132 is in the digital image or video 104 is in the range of 0.5 to 0.9, depending on the particular photographer 132.

FIG. 4 shows a more detailed view of the individual recognition classifier 114. For each set of personal features 110 extracted by the person finder 106 a comparer 140 compares the personal features 110 with each of the M appearance models $116_{1\text{-}M}$ representing M individuals of interest and outputs a score set 142 of M scores indicating the likelihood or probability that the particular person found by the person finder is the mth person of interest. The comparer 140 can for example calculate a Euclidean distance between the personal features 110 and each of the M appearance models. Or the comparer 140 can compute a Mahalanobis distance from each of the M appearance models to produce the score set 142. Further, the comparer 140 can be any classifier, such as but not limited to, Gaussian Maximum Likelihood, a neural network, a support vector machine or the like. Preferably, the mth entry of the score set 142 indicates

the probability that the particular face corresponding to the set of personal features 110 is the mth person of interest.

The score set 142 is passed to a score adjuster 144 for adjusting the score according to information related to the photographer 132 and the capture information 112, producing an adjusted score set. The score adjuster 144 considers the score set likelihoods or probabilities and refines the scores as follows. The scores in the score set 142 are adjusted according to the capture information 112. When the capture information 112 indicates that the self-timer flag was used to capture the digital image or video 104, then the score for the mth person of interest is increased if the mth person is the photographer 132 of the digital image or video 104. In this manner, the score adjuster 144 considers the prior probability (i.e. the prior probability of an event A is the probability that A occurs in the absence of any other data) of the photographer 132 appearing in the digital image or video 104 when the self-timer is user to capture the digital image or video 104. Likewise, when the capture information 112 indicated that the digital image or video 104 was captured using a remote signal to activate the camera's capture mechanism, the score for the mth person of interest is increased if the mth person is the photographer 132 of the digital image or video 104. The score adjuster 144 outputs a person classification 118 for the person detected by the person finder 106. The person classification 118 can be the score set 142 after the adjustment by the score adjuster 144. Or the person classification 118 can be the identity of the person of interest with the highest corresponding score in the adjusted score set, providing that that score is greater than a threshold T0.

Conceptually, to produce the person classification 118, the individual recognition classifier 114 preferably computes:

$P(x = m \mid f)$, i.e. the probability that the person detected by the person finder 106 is person m, given the evidence of the personal features 110 f. By Bayes rule,

This quantity can be computed for each of the m persons of interest by:

$$P(x = m \mid f) = P(f \mid x = m)\, P(x = m) / P(f)$$

The term $P(f \mid x = m)$ is the probability of observation of the personal features f when it is known the person is the mth person of interest. This can be found by considering appearance model 116 for the mth person of interest which describes the variation in appearance for the mth person of interest. The term P(x=m) is the prior probability and is the probability that a person in an image or video is the person of interest m. The prior probability varies as a function of the identity of the photographer 132. For example, a wife and husband share a camera. Of the people appearing in images where the wife is the photographer, 60% are the baby, 20% are the husband, and 20% are others. When the husband is the photographer, 40% of the people appearing in photos are the baby, 20% are the wife, 5 % are the husband, and 35% are others. Therefore, when the individual recognition classifier 114 knows the identity of the photographer 132, a photographer content profile 130 associated with that photographer 132 can be used by the score adjuster 144 to properly adjust the score set 142 in an appropriate fashion. In the preferred embodiment, the photographer content profile 130 contains the prior probabilities of persons of interest appearing in images and videos for a particular photographer. Preferably, the score set 142 contains the probabilities $P(f \mid x = m)$ and the score adjuster 144 adjusts the scores by multiplicatively weighting with the prior probability $P(x=m)$ specified in the photographer content profile 130.

The photographer content profiles 130 for a particular photographer are generated by having a user manually verify the identities of people in a set of images or videos captured by the particular photographer. Then the prior probabilities are computed and stored in the photographer content profile 130. The prior probabilities can consider the capture information 112. For example, a photographer 132 has one set of prior probabilities that describe the probability of a person being the mth person of interest when the self-timer function is on as indicated by the capture information 112, and a second set of prior probabilities with the self-timer function is off. For example, the following table gives the prior probabilities that a given person in an image or video is the mth person of interest for two different photographers and when the self-timer function is off and on.

	Photographer is person of interest 0		Photographer is person of interest 1	
Mth Person of interest	Self-timer on	Self-timer off	Self-timer on	Self-timer off
0	0.3	0.0	0.3	0.2
1	0.3	0.3	0.3	0.0
2	0.2	0.4	0.3	0.6
unknown	0.2	0.3	0.1	0.2

Therefore, the photographer 132 of the digital image or video 104 is identified along with capture information 112 related to the digital image or video 104. The photographer content profile 130 corresponding to the photographer 132 is used to determine the identities of persons in the digital image or video 104.

FIG. 5 shows an alternative embodiment for using the identify of the photographer 132 to identify objects within the digital image or video 104 or to classify the digital image or video itself. Digital images or videos 104 from a collection are passed to a feature extractor 152 for extracting features 160 that are passed to an object classifier 164.

Additionally, the appearance models for objects of interest $117_{1\text{-}M}$ are passed to the object classifier. A comparer 140 compares the features 160 extracted from the images or videos with the appearance models of the objects of interest $117_{1\text{-}M}$, producing the score set 142. Preferably, the score set 142 includes a probability that the features 160 relate to a particular object *m* of interest.

The identity of the photographer 132 and capture information 112 is passed to the score adjuster 144. The score adjuster 144 loads a photographer content profile 130 that describes the prior probability of the particular object m is in the image or video and adjusts the score set 142 accordingly to produce an adjusted score set, resulting in a classification 118 that is stored in a database 120, ready for querying as before. Alternatively, the photographer content profile 130

describes the prior probability that the image is an object of interest. The photographer content profile 130 associated with the photographer 132 describes the probability that the image represents the object of interest.

For example, the object classifier 164 can have the objective of determining whether an image is an "indoor" or "outdoor" image. However, different photographers capture different proportions of their images indoor versus outdoor. For example, photographer 0 captures 30 % indoor images and 70% outdoor images but photographer 1 captures 30% indoor images and 70% outdoor images. This information is provided by the photographer content profile 130 corresponding to the identify of the photographer 132. Thus, knowledge of the prior probability for a particular photographer allows the score adjuster 144 to adequately consider the prior probability and improve the overall performance of the object classifier 164.

The object classifier 164 in this example classifies the state of the image as either an indoor or an outdoor image. Other object classifiers 164 can be used to determine whether an image is a natural scene or a manmade scene. Furthermore, an object classifier 164 can be used to determine if an image is a sunset image or not a sunset image.

The object classifier 164 can also be used to find specific objects within an image. For example, the individual recognition classifier 114 is an example of an object classifier used to recognize individual objects within a scene. In another embodiment, the object classifier 164 is used to detect the presence of a redeye defect (which may occur 0, 1 or many times in a single image). The object classifier 164 determines whether an image represents the object of interest.

Furthermore, the photographer content profile 130 can be dependent on the capture information 112 in addition to the identify of the photographer 132. For example, the following table is a photographer content profile 130 and shows the probability that a given image or video captured by a given photographer is "indoor" or "outdoor", as based on the month of the image capture that is contained in the capture information 112. In this case, "indoor" and "outdoor" are objects of interest that are described with an appearance model used

by the object classifier 164 to classify an image as an indoor image or an outdoor image.

	Photographer 0		Photographer 1	
	indoor	Outdoor	indoor	outdoor
Jan-March	0.3	0.7	0.5	0.5
April-June	0.5	0.5	0.3	0.7
July-Sept.	0.6	0.4	0.2	0.8
Oct.-Dec	0.4	0.6	0.8	0.2

The photographer content profile 130 has been shown to include prior probability information for the classification of a single image or video. Additionally, the photographer content profile 130 can contain information related to the probability of a particular image (or video) being outdoors given that a previous image was outdoors for example. This information is stored as a state transition matrix as are commonly used in the study of Markov Chains and hidden Markov Models. The state transition matrices are dependent on the identification of the photographer, because they are related to the photographic behavior of that individual. For example, a state transition matrix for photographer 2:

	For photographer 2 Probability image or video n+1 is	
When image n is:	indoor	Outdoor
indoor	0.8	0.2
outdoor	0.3	0.7

The transition matrix is a special case of a prior probability. The transition matrix can depend on the capture information 112, for example the time interval between the image n and the image n+1. For example, if the time interval between the two images is large (e.g. 3 days), then the state transition matrix is:

	For photographer 2 Probability image or video n+1 is	
When image n is:	indoor	Outdoor
indoor	0.6	0.4
outdoor	0.43	0.57

Once the correction photographer content profile 130 is known, hidden Markov models can be used along with the state transition matrix to determine the state of the image (in this case, whether the image is indoor or outdoor.)

The capture information 112 and identify of the photographer 132 are used to select the correct photographer content profile 130 for inputting to the object classifier 164. In a further embodiment, knowing the identity of the photographer further enables a more accurate image orientation detection. In general, a rectangular image is properly viewed in one of four possible viewing orientations. Luo, in U.S. Patent Application Publication US 2003/0152289 A1 teaches a method to automatically determination which of these four orientations is correct for an image based on semantic object and scene layout detections and employing an arbitration method to estimate of image orientation. The prior probabilities of horizontal, vertical 1, vertical 2, and upside down horizontal are noted to be 70%-14%-14%-2%. FIG. 6A shows an example of an image in horizontal orientation. FIGS. 6B-6D show image having orientations of vertical 1, vertical 2, and upside down horizontal, respectively.

Generally, photographers capture landscape scenes in the horizontal orientation (i.e. photographers rarely hold the camera upside down when photographing a scene). However, for vertical or portrait scenes with an aspect ratio having larger height than width, there are two possible camera orientations. Most photographers take "vertical" photographs using only one of these positions.

Knowing the photographer's identity establishes that photographer's individual behavior, thus improving its performance in determining image orientation.

An example orientation probability versus photographer matrix (the photographer probability profile 130 of FIG. 5) is shown below:

	Photographer 0	Photographer 1
Horizontal	0.850	0.650
Upside Down	0.005	0.010
Vertical 1	0.125	0.030
Vertical 2	0.020	0.310

Having improved image orientation determination performance improves the performance of subsequent image understanding algorithms that utilize a priori knowledge of orientation. Knowledge of other photographer specific capture traits (types of scenes, camera settings, typical location and time of capture) provides additional information that can improve the performance of subsequent image enhancement, image organization, and image management algorithms. For example, knowing if a photographer does not have a steady hand (resulting in excessive camera motion during image capture), could signal a subsequent image enhancement algorithm to more aggressively attempt to correct for image blur. Yet another example is if a particular photographer tends to not keep the camera level with the horizon, knowing the photographer identity could signal an image enhancement algorithm that levels the image.

PARTS LIST

10 image capture devices
20 microprocessor-based unit (aka digital image processor)
30 image output device
40 general control computer
50 display device
60 keyboard
70 offline memory device
104 digital images or videos
106 person finder
108 information extractor
110 personal features
112 capture information
114 individual recognition classifier
116 appearance model of a person of interest
117 objects of interest
118 person classification
120 database
122 query or queried
124 query results
130 photographer content profile
132 photographer
138 photographer determiner
140 comparer
142 score set
144 score adjuster
160 features
164 object classifier

CLAIMS:

1. A method of identifying at least one particular person of interest in a collection of digital images taken over time, comprising:

providing the collection of digital images with each digital image containing one or more persons;

storing in a digital database an appearance model having a set of features associated with the particular person of interest and a prior probability of the person of interest appearing in images by a particular photographer; and

comparing the appearance model with features extracted from the digital images in the collection of digital images and using the prior probability and the appearance model to determine if the particular person of interest is in one or more digital images in the collection of digital images.

2. The method of claim 1 wherein the particular person of interest is the photographer and further including providing image capture information relating to the camera settings used by the particular photographer to change the prior probability of the particular photographer being in the collection of digital images.

3. The method of claim 2 wherein the image capture information further includes the mode of the camera self-timer.

4. The method of claim 3 wherein the prior probability is increased when the person of interest is the photographer and the mode of the camera self-timer is on.

5. The method of claim 3 wherein the prior probability is decreased when the person of interest is the photographer and the mode of the camera self-timer is off.

6. The method of claim 3 wherein the prior probability is increased when the person of interest is other than the particular photographer.

7. A method of classifying an image, comprising:

providing a collection of digital images taken by a particular photographer;

storing in a digital database an appearance model having a set of features associated with an object of interest;

providing a photographer content profile associated with the photographer describing the probability that the image represents the object of interest; and

using the appearance model and the photographer content profile to classify the digital image in the collection.

8. The method of claim 7 further including providing image capture information relating to the camera settings used by the particular photographer.

9. The method of claim 7 wherein the photographer content profile includes information related to the distribution of digital image orientation of digital images taken by the photographer.

10. The method of claim 9, wherein image content in the digital image of interest and the photographer content profile is used to determine the orientation of the digital image of interest.

11. The method of claim 7 wherein the photographer content profile includes information related to the distribution of digital images being captured indoors or outdoors when taken by the photographer.

12. The method of claim 11, wherein image content in the digital image of interest and the photographer content profile is used to determine the whether the digital image of interest is an indoor or an outdoor image.

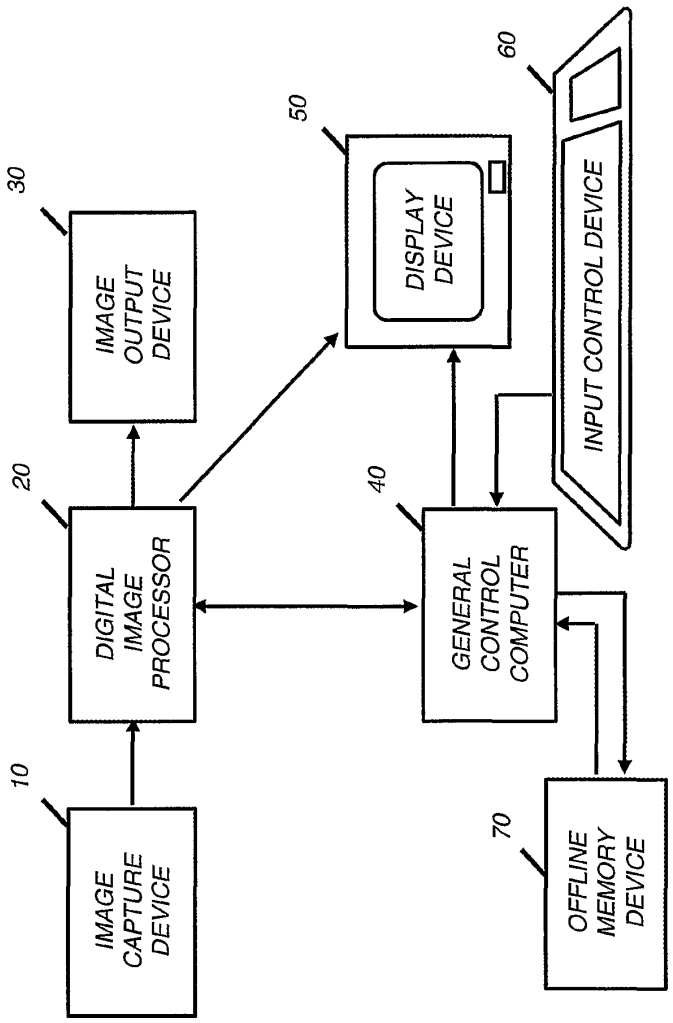


IMAGE CAPTURE DEVICE
10
DIGITAL IMAGE PROCESSOR
20
IMAGE OUTPUT DEVICE
30
DISPLAY DEVICE
50
GENERAL CONTROL COMPUTER
40
INPUT CONTROL DEVICE
60
OFFLINE MEMORY DEVICE
70

FIG. 1

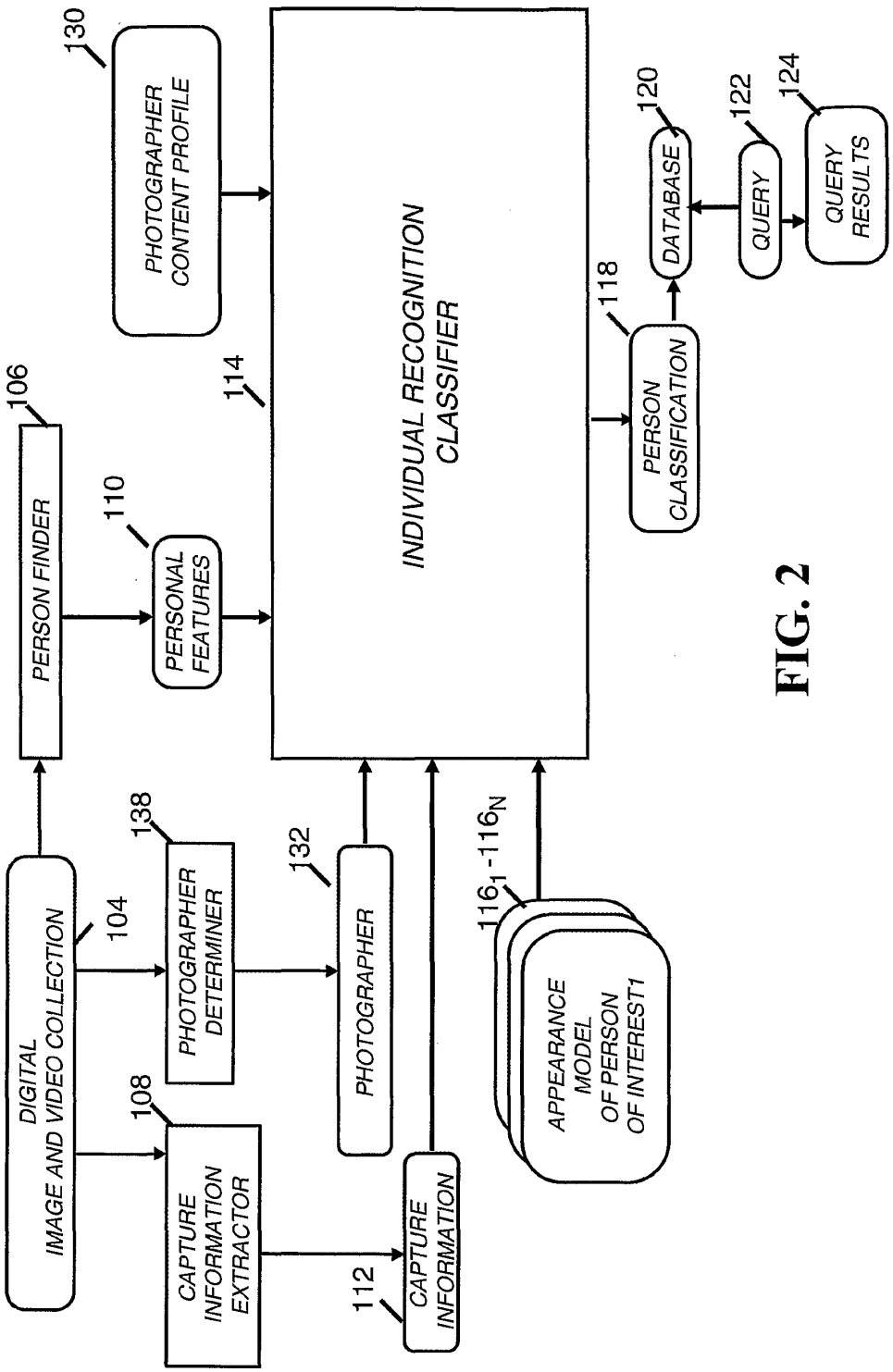

DIGITAL IMAGE AND VIDEO COLLECTION
104
PERSON FINDER
106
PHOTOGRAPHER DETERMINER
138
CAPTURE INFORMATION EXTRACTOR
108
PERSONAL FEATURES
110
PHOTOGRAPHER
132
CAPTURE INFORMATION
112
PHOTOGRAPHER CONTENT PROFILE
130
INDIVIDUAL RECOGNITION CLASSIFIER
114
APPEARANCE MODEL OF PERSON OF INTEREST1
116$_1$-116$_N$
PERSON CLASSIFICATION
118
DATABASE
120
QUERY
122
QUERY RESULTS
124

FIG. 2

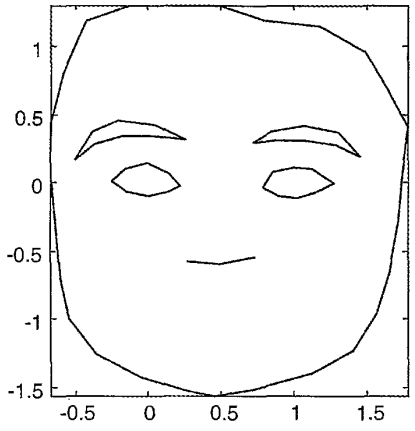


FIG. 3A

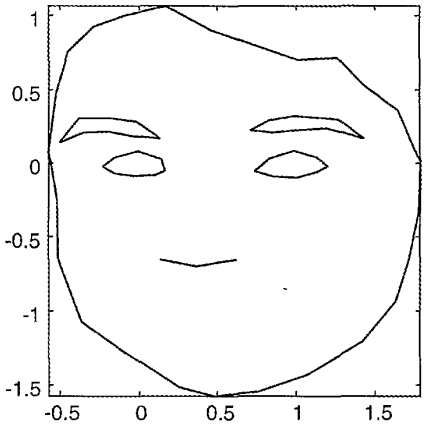


FIG. 3B

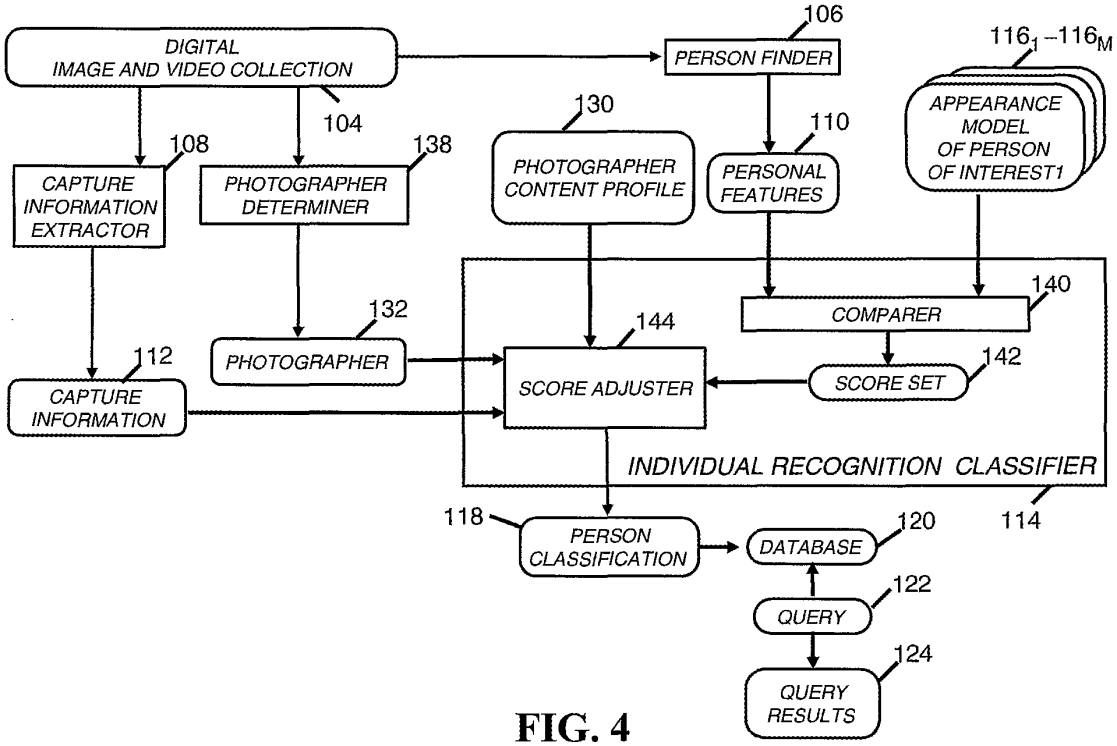

DIGITAL IMAGE AND VIDEO COLLECTION
104
106
PERSON FINDER
116$_1$ –116$_M$
APPEARANCE MODEL OF PERSON OF INTEREST1
108
CAPTURE INFORMATION EXTRACTOR
138
PHOTOGRAPHER DETERMINER
130
PHOTOGRAPHER CONTENT PROFILE
110
PERSONAL FEATURES
140
COMPARER
132
PHOTOGRAPHER
144
SCORE ADJUSTER
142
SCORE SET
112
CAPTURE INFORMATION
INDIVIDUAL RECOGNITION CLASSIFIER
114
118
PERSON CLASSIFICATION
120
DATABASE
122
QUERY
124
QUERY RESULTS

FIG. 4

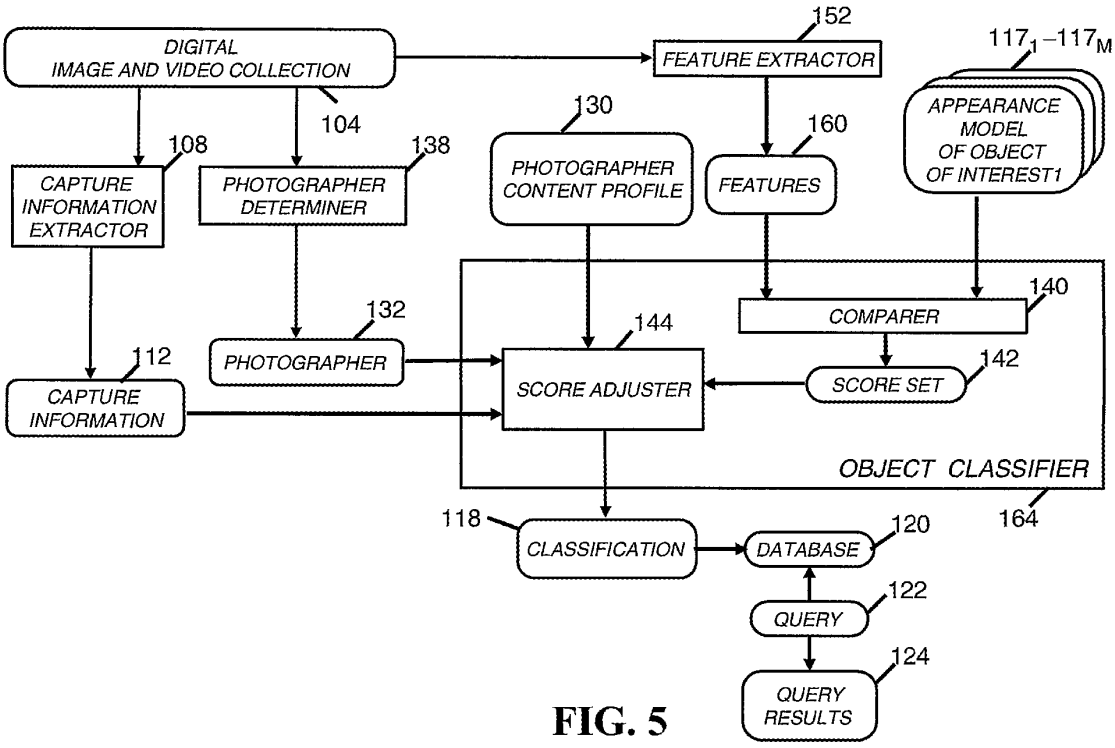

DIGITAL IMAGE AND VIDEO COLLECTION
104
152
FEATURE EXTRACTOR
117_1–117_M
APPEARANCE MODEL OF OBJECT OF INTEREST1
130
PHOTOGRAPHER CONTENT PROFILE
160
FEATURES
108
CAPTURE INFORMATION EXTRACTOR
138
PHOTOGRAPHER DETERMINER
140
COMPARER
132
PHOTOGRAPHER
144
SCORE ADJUSTER
142
SCORE SET
112
CAPTURE INFORMATION
OBJECT CLASSIFIER
164
118
CLASSIFICATION
120
DATABASE
122
QUERY
124
QUERY RESULTS

FIG. 5

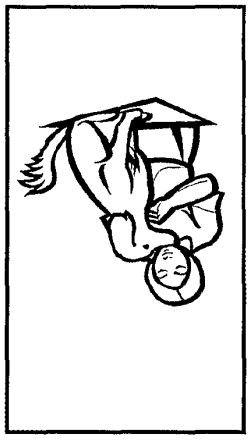


FIG. 6B

FIG. 6D

FIG. 6A

FIG. 6C

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/020712

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06K9/00
ADD. G06F17/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06K G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DAVIS M ET AL.: "From Context to Content: Leveraging Context to Infer Media Metadata" PROC. ACM INT. CONF. ON MULTIMEDIA (MM'04), 10 October 2004 (2004-10-10), - 16 October 2004 (2004-10-16) pages 188-195, XP002395035 the whole document	1,2,7-12
Y	US 2004/170323 A1 (COOTES TIMOTHY F ET AL) 2 September 2004 (2004-09-02) abstract	1,2,7-12
Y	US 2002/140843 A1 (TRETTER DANIEL R ET AL) 3 October 2002 (2002-10-03) abstract; figure 3 paragraph [0025] - paragraph [0026]	2,8,11, 12

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 August 2006	08/09/2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Müller, M

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	BOUTELL M ET AL: "Bayesian fusion of camera metadata cues in semantic scene classification" COMPUTER VISION AND PATTERN RECOGNITION, 2004. CVPR 2004. PROCEEDINGS OF THE 2004 IEEE COMPUTER SOCIETY CONFERENCE ON WASHINGTON, DC, USA 27 JUNE - 2 JULY 2004, PISCATAWAY, NJ, USA,IEEE, 27 June 2004 (2004-06-27), pages 1-8, XP002319660 ISBN: 0-7695-2158-4 the whole document	2,8,11, 12
Y	EP 1 418 509 A (EASTMAN KODAK COMPANY) 12 May 2004 (2004-05-12) paragraph [0028] - paragraph [0044]; table 2	9,10
A	LEI ZHANG ET AL: "Automated annotation of human faces in family albums" PROCEEDINGS OF THE 11TH. ACM INTERNATIONAL CONFERENCE ON MULTIMEDIA. MM'03. BERKELEY, CA, NOV. 4 - 6, 2003, ACM INTERNATIONAL MULTIMEDIA CONFERENCE, NEW YORK, NY : ACM, US, vol. CONF. 11, 2 November 2003 (2003-11-02), pages 355-358, XP002361520 ISBN: 1-58113-722-2 abstract	1-12
A	LONGBIN CHEN ET AL: "Face annotation for family photo management" INTERNATIONAL JOURNAL OF IMAGE AND GRAPHICS, WORLD SCIENTIFIC PUBLISHING CO., SINGAPORE, SG, vol. 3, no. 1, 30 December 2002 (2002-12-30), pages 81-94, XP002361519 ISSN: 0219-4678 abstract page 1 - page 4	1-12

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2006/020712

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004170323 A1	02-09-2004	CA 2448448 A1	05-12-2002
		EP 1393243 A1	03-03-2004
		WO 02097720 A1	05-12-2002
		JP 2004527863 T	09-09-2004
US 2002140843 A1	03-10-2002	EP 1374096 A2	02-01-2004
		JP 2005510775 T	21-04-2005
		WO 02082328 A2	17-10-2002
EP 1418509 A	12-05-2004	US 2004120572 A1	24-06-2004

Form PCT/ISA/210 (patent family annex) (April 2005)

Espacenet

Bibliographic data: WO2008107002 (A1) — 2008-09-12

FACE SEARCHING AND DETECTION IN A DIGITAL IMAGE ACQUISITION DEVICE

Inventor(s): STEINBERG ERAN [US]; BIGIOI PETRONEL [RO]; CORCORAN PETER [IE]; GANGEA MIHNEA [RO]; PETRESCU STEFAN MIREL [RO]; VASILIU ANDREI [RO]; COSTACHE GABRIEL [IE]; DRIMBAREAN ALEXANDRU [IE] + (STEINBERG, ERAN, ; BIGIOI, PETRONEL, ; CORCORAN, PETER, ; GANGEA, MIHNEA, ; PETRESCU, STEFAN, MIREL, ; VASILIU, ANDREI, ; COSTACHE, GABRIEL, ; DRIMBAREAN, ALEXANDRU)

Applicant(s): FOTONATION VISION LTD [IE]; STEINBERG ERAN [US]; BIGIOI PETRONEL [RO]; CORCORAN PETER [IE]; GANGEA MIHNEA [RO]; PETRESCU STEFAN MIREL [RO]; VASILIU ANDREI [RO]; COSTACHE GABRIEL [IE]; DRIMBAREAN ALEXANDRU [IE] + (FOTONATION VISION LIMITED, ; STEINBERG, ERAN, ; BIGIOI, PETRONEL, ; CORCORAN, PETER, ; GANGEA, MIHNEA, ; PETRESCU, STEFAN, MIREL, ; VASILIU, ANDREI, ; COSTACHE, GABRIEL, ; DRIMBAREAN, ALEXANDRU)

Classification: **- international:** ***G06K9/00***
- cooperative: **G06K9/00221**; **G06K9/00228**; **G06K9/00234**; **G06K9/00241**; **G06K9/00268**; **G06K9/00288**

Application number: WO2007EP06540 20070723

Priority number(s): US20070892883P 20070305

Also published as: US2016104032 (A1) US2015169941 (A1) US9224034 (B2) US2014153780 (A1) US8923564 (B2) more

Abstract of WO2008107002 (A1)

First page clipping of WO2008107002 (A1)

A method of detecting a face in an image includes performing face detection within a first window of the image at a first location. A confidence level is obtained from the face detection indicating a probability of the image including a face at or in the vicinity of the first location. Face detection is then

performed within a second window at a second location, wherein the second location is determined based on the confidence level.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 September 2008 (12.09.2008)

PCT

(10) International Publication Number
WO 2008/107002 A1

(51) International Patent Classification:
G06K 9/00 (2006.01)

(21) International Application Number:
PCT/EP2007/006540

(22) International Filing Date: 23 July 2007 (23.07.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/892,883 5 March 2007 (05.03.2007) US

(71) Applicant *(for all designated States except US)*: **FOTONATION VISION LIMITED** [IE/IE]; Galway Business Park, Dangan, Galway (IE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **STEINBERG, Eran** [IL/US]; 137 Granville Way, San Francisco, CA 94127 (US). **BIGIOI, Petronel** [RO/RO]; 57 Sceilg Ard, Headford Road, County Galway (IE). **CORCORAN, Peter** [IE/IE]; Cregg, Claregalway, Galway (IE). **GANGEA, Mihnea** [RO/RO]; Sos. Nicolae Titulescu Nr. 10, Bloc 20, Scara A et 9, Ap. 44, Sector 1, Bucuresti (RO). **PETRESCU, Stefan, Mirel** [RO/RO]; Bl.73, sc.3, et.2, ap.37, Str. Cap, Gheorghe Ion, Nr.4, Sector 4, Mun.Bucuresti (RO). **VASILIU, Andrei** [RO/RO]; Str. Armenis Nr. 8-10. Bl. J5, Apt. 84, Sector 3, Bucuresti (RO). **COSTACHE, Gabriel** [RO/IE]; 19 Lui Na Greine, Knocknacarra, Galway (IE). **DRIMBAREAN, Alexandru** [RO/IE]; 60 Garraun Ard, Doughiska, Galway (IE).

(74) Agents: **CONOR, Boyce** et al.; F.R. Kelly & Co., 27 Clyde Road, Ballsbridge, Dublin 4 (IE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[Continued on next page]

(54) Title: FACE SEARCHING AND DETECTION IN A DIGITAL IMAGE ACQUISITION DEVICE

(57) Abstract: A method of detecting a face in an image includes performing face detection within a first window of the image at a first location. A confidence level is obtained from the face detection indicating a probability of the image including a face at or in the vicinity of the first location. Face detection is then performed within a second window at a second location, wherein the second location is determined based on the confidence level.

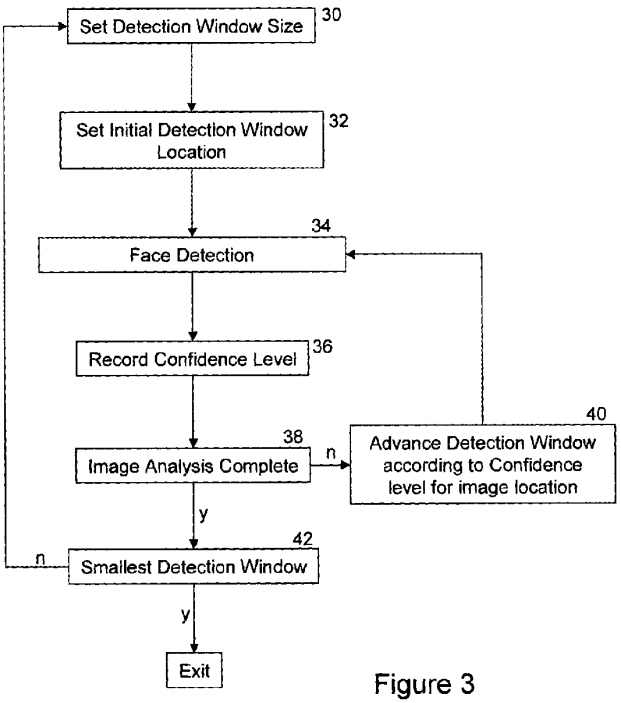


Figure 3

WO 2008/107002 A1

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

FACE SEARCHING AND DETECTION IN A DIGITAL IMAGE ACQUISITION DEVICE

FIELD OF THE INVENTION

The present invention provides an improved method and apparatus for image processing in digital image acquisition devices. In particular the invention provides improved performance and accuracy of face searching and detection in a digital image acquisition device.

BACKGROUND OF THE INVENTION.

Several applications such as US published application no. 2002/0102024 to inventors Jones and Viola relate to fast-face detection in digital images and describe certain algorithms. Jones and Viola describe an algorithm that is based on a cascade of increasingly refined rectangular classifiers that are applied to a detection window within an acquired image. Generally, if all classifiers are satisfied, a face is deemed to have been detected, whereas as soon as one classifier fails, the window is determined not to contain a face.

An alternative technique for face detection is described by Froba, B., Ernst, A., "Face detection with the modified census transform", in Proceedings of 6th IEEE Intl. Conf. on Automatic Face and Gesture Recognition, 17-19 May 2004 Page(s): 91 – 96. Although this is similar to Viola-Jones each of the classifiers in a cascade generates a cumulative probability and faces are not rejected if they fail a single stage of the classifier. We remark that there are advantages in combining both types of classifier (i.e. *Viola-Jones* and *modified census*) within a single cascaded detector.

Figure 1 illustrates what is described by Jones and Viola. For an analysis of an acquired image 12, the detection window 10 is shifted incrementally by dx pixels across and dy pixels down until the entire image has been searched for faces 14. The rows of dots 16 (not all shown) represent the position of the top-left corner of the detection window 10 at each face detection position. At each of these positions, the classifier chain is applied to detect the presence of a face.

Referring to Figures 2a and 2b, as well as investigating the current position, neighboring positions can also be examined, by performing small oscillations around the current detection window and/or varying slightly a scale of the detection window. Such

CONFIRMATION COPY

oscillations may vary in degree and in size creating consecutive windows with some degree of overlap between an original window and a second window. The variation may also be in the size of the second window.

A search may be performed in a linear fashion with the dx,dy increments being a pre-determined function of image resolution and detection window size. Thus, the detection window may be moved across the image with constant increments in x and y directions.

A problem with linear searching occurs when the window size decreases, such as when attempting to detect small faces, and the number of sliding windows that are to be analyzed increases quadratically to the reduction in window size.. This results in a compounded slow execution time, making "fast" face detection otherwise unsuitable for real-time embedded implementations.

US Application No. 11/464,083, filed August 11, 2006, which is assigned to the same assignee as the present application, discloses improvements to algorithms such as those described by Jones and Viola, and in particular in generating a precise resolution corresponding to a representation of an image, such as an integral image or a Gaussian image, for subsequent face detection.

SUMMARY OF THE INVENTION

A method of detecting a face in an image includes performing face detection within a first window of the image at a first location. A confidence level is obtained from the face detection indicating a probability of the image including a face at or in the vicinity of the first location. Face detection is performed within a second window at a second location that is determined based on the confidence level.

A number of windows that are analyzed is advantageously significantly reduced for a same face detection quality, and so faster face searching is provided, even in the case of small faces, therefore allowing acceptable performance for face detection in real-time embedded implementations such as in digital cameras, mobile phones, digital video cameras and hand-held computers.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 illustrates schematically an image being processed by a conventional face detection process;

Figure 2(a) illustrates a detection window oscillating diagonally around an initial position;

Figure 2(b) illustrates a smaller scale detection window oscillating transversely around the initial position;

Figure 3 is a flow diagram of a method of face searching and detection according to a preferred embodiment;

Figure 4 illustrates schematically an image being processed according to a preferred embodiment; and

Figure 5 is a flow diagram illustrating post-processing of a detected face region prior to face recognition.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

An improved method of face searching and detection in a digital image acquisition device is described that calculates x and/or y increments of a detection window in an adaptive fashion.

In face detection processes, during analysis of a detection window and/or while oscillating around the detection window, a confidence level can be accumulated providing a probabilistic measure of a face being present at the location of the detection window. When the confidence level reaches a preset threshold for a detection window, a face is confirmed for location of the detection window.

Where a face detection process generates such a confidence level for a given location of detection window, in a preferred embodiment, the confidence level is captured and stored as an indicator of the probability of a face existing at the given location. Such probability may reflect confidence that a face has been detected, or confidence that there is no face detected in the window.

Alternatively, where a face detection process applies a sequence of tests each of which produce a Boolean "Face" or "No face" result, the extent to which the face detection process has progressed through the sequence before deciding that no face exists at the

location can be taken as equivalent to a confidence level and indicating the probability of a face existing at the given location. For example, where a cascade of classifiers fails to detect a face at a window location at classifier 20 of 32, it could be taken that this location is more likely to include a face (possibly at a different scale or shifted slightly) than where a cascade of classifiers failed to detect a face at a window location at classifier 10 of 32.

Referring now to Figure 3, face searching and detection according to one embodiment, begins by selecting the largest size of detection window at step 30 and positioning the window at the top left corner of an image at step 32.

Alternatively, if particular regions of an image have been identified through some pre-processing as being more likely to include a face, the detection window can be located at a suitable corner of one such region and the embodiment can be applied to each such region of the image in turn or in parallel. Examples of such pre-processing include identifying regions of the image which include skin as being candidate face regions.

In this regard, it is possible to create a skin map for an acquired image where the value of a pixel within the skin map is determined by its probability of being a skin pixel.

There are many possible techniques for providing a skin map, for example:

(i) "Comparison of Five Color Models in Skin Pixel Classification", Zarit et al presented at ICCV '99 International Workshop of Recognition, Analysis, and Tracking of Faces and Gestures in Real-Time Systems, contains many references to tests for skin pixels;

(ii) U.S. Pat. No. 4,203,671, Takahashi et al., discloses a method of detecting skin color in an image by identifying pixels falling into an ellipsoid in red, green, blue color space or within an ellipse in two dimensional color space;

(iii) US Pat. No. 7,103,215 describes a method of detecting pornographic images, wherein a color reference database is prepared in LAB color space defining a plurality of colors representing relevant portions of a human body. A questionable image is selected, and sampled pixels are compared with the color reference database. Areas having a matching pixel are subjected to a texture analysis to determine if the pixel is an isolated color or if other comparable pixels surround it; a condition indicating possible skin;

(iv) US 11/624,683 filed January 18, 2007 (Ref: FN185) discloses real-valued skin tests for images in RGB and YCC formats. So, for example, where image information is available in RGB format, the probability of a pixel being skin is a function of the degree to which L exceeds 240, where L=0.3*R+0.59G+0.11B, and/or the degree to which R exceeds G + K and R exceeds B + K where K is a function of image saturation. In YCC format, the

probability of a pixel being skin is a function of the degree to which Y exceeds 240, and/or the degree to which Cr exceeds 148.8162 – 0.1626*Cb + 0.4726*K and Cr exceeds 1.2639*Cb – 33.7803 + 0.7133*K, where K is a function of image saturation.

It will also be understood that many different techniques exist to provide a binary skin/not-skin classification (typically based on simple thresholding). So, it can be understood that some pixels may qualify as skin under one binary technique and as not-skin under a second technique. So in alternative implementations, several binary techniques can be combined, so that pixels may be ranked according to a number of criteria to obtain a relative probability that any particular pixel is skin. It is advantageous to weight different skin detection techniques according to image capture conditions, or according to data analyzed from previous image frames.

Where multiple skin classification techniques are implemented in a parallel hardware architecture it becomes possible to combine to outputs of multiple skin classification techniques in a single analysis step, quickly generating a refined skin probability for each image pixel as it become available from the imaging sensor. In one preferred embodiment this refined skin probability is represented as a grayscale value, 2^N where N>1 (N=1 represents a simple binary mask of skin/not-skin). In any case, once an image pixel is classified by a non-binary algorithm it may be considered as a grayscale representation of skin probability.

In assessing whether various sizes and locations of windows in an image might include portions of skin, it can be advantageous to use the integral image techniques disclosed in US 2002/0102024, Viola-Jones with the skin map probability values produced for an image.

In such an integral image, each element is calculated as the sum of intensities i.e. skin probabilities of all points above and to the left of the point in the image. The total intensity of any sub-window in an image can then be derived by subtracting the integral image value for the top left point of the sub-window from the integral image value for the bottom right point of the sub-window. Also intensities for adjacent sub-windows can be efficiently compared using particular combinations of integral image values from points of the sub-windows.

Thus the techniques employed to construct an integral image for determining the luminance of a rectangular portion of the final image may equally be employed to create a skin probability integral image. Once this integral image skin map (IISM) is created, it enables the skin probability of any rectangular area within the image to be quickly

determined by simple arithmetic operations involving the four corner points of the rectangle, rather than having to average skin values over the full rectange.

In the context of a fast face detector as described in the remainder of this specification, it can be understood that obtaining a rapid calculation of the averaged local skin pixel probability within a sub-window enables the skin probability to be advantageously employed either to confirm a local face region, or to be used as an additional, color sensitive classifier to supplement conventional luminance based Haar or census classifiers.

Alternatively or in combination with detection of skin regions, where the acquired image is one of a stream of images being analyzed, the candidate face regions might be face regions detected in previous frames, such as may be disclosed at US Application No. 11/464,083, (Ref: FN143) filed August 11, 2006.

Figure 2a illustrates the detection window oscillating diagonally around an initial position (outlined in bold). Figure 2b illustrates a smaller scale detection window oscillating transversely around the initial position before further face detection is performed. These oscillations dox,doy and scale changes ds are typically smaller that the dx,dy step of the detection window. A decision as to scale of oscillation depends on results of applying the search algorithm on the initial window. Typically, a range of about 10-12 different sizes of detection window may be used to cover the possible face sizes in an XVGA size image.

Returning to the operation of the main face detector, we note that ace detection is applied for the detection window at step 34, and this returns a confidence level for the detection window. The particular manner in which the detection window oscillates around a particular location and the calculation of the confidence level in the preferred embodiment is as follows:

Once a given detection window location has been tested for the presence of a face, the window is sequentially shifted by –dox,-doy; +dox,-doy; +dox,+doy; and –dox,-doy (as shown in Figure 2(a)) and tested at each of these four locations. The confidence level for the window location and four shifted locations is accumulated. The confidence level may then be ported to each new window based on the new window size and location. If a target face-validation confidence threshold is not reached, the detection window is shrunk (indicated by ds). This smaller detection window is tested, then sequentially shifted by –dox,0; +dox,0; 0,+doy; and 0,-doy (as shown in Figure 2(b)) and tested at each of these four locations. The confidence level for these five locations of the smaller scale detection window is added to the previous confidence level from the larger scale window.

The confidence level for the detection window location is recorded at step 36.

If the detection window has not traversed the entire image/region to be searched at step 38, it is advanced as a function of the confidence level stored for the location at step 40.

In the preferred embodiment, where the confidence level for an immediately previous detection window at the present window size has exceeded a threshold, then the x and y increment for the detection window is decreased.

Referring now to Figure 4, which shows how in the preferred embodiment, the shift step is adjusted when the confidence level for a location signals the probability of a face in the vicinity of the location. For the first four rows of searching, a relatively large increment is employed in both x and y directions for the detection window. For the location of detection window 10(a), however, it is more than likely that the oscillation of the window in the bottom-right direction will provide the required confidence level of the face 14 being at the location. As such, the increment for the detection window in the x and y directions is decreased. In the example, the confidence level will remain above the determined threshold until the detection window location passes to the right of the line tl2. At this time, the x increment reverts to the original large increment. Having incremented by the small increment in the y direction, the detection window is advanced on the next row with a large x increment until it reaches the line tl1. Either because the confidence level for this location will again exceed the required threshold or indeed because it did for the previous row, the x increment is again decreased until again the detection window passes to the right of the line tl2. This process continues until the detection window arrives at location 10(b). Here, not alone is the confidence level for increased resolution face detection reached, but the face 14 is detected. In the preferred embodiment, this causes both the x and y increments to revert to original large increments.

If a face is not detected in a region following a confidence level triggering at a face-like (but not an actual face) position, the x and y increments return to their original relaxed value, when over the whole extent of a row, the confidence levels do not rise above the threshold level. So for example, in the row after the detection window passes location 10(c), no detection window will produce a confidence level above the threshold and so after this row, the y increment would revert to its relaxed level, even if a face had not been detected at location 10(b).

Once the image and/or its regions have been traversed by a detection window of a given size, unless this has been the smallest detection window at step 42 of Figure 3, the next smallest detection window is chosen at step 30, and the image traversed again.

In certain embodiments, when the confidence level for an immediately previous detection window at the present window size exceeds a threshold, a change in dx,dy for a detection window is triggered. However, this change could equally and/or additionally be a function of or be triggered by the confidence level for a bigger detection window or windows at or around the same location.

In certain embodiments, detection windows are applied from the largest to the smallest size and so it is assumed that a given location has been checked by a larger sized detection window before a given sized detection window, so indicating that if a face has not been detected for the larger sized detection window, it is to be found near that location with a smaller sized detection window. Alternatively, it can indicate that even if a face has been found at a given location for a larger sized detection window, there is a chance that the face might be more accurately bounded by a smaller sized detection window around that location when subsequently applied.

As many more windows may be employed when looking for smaller size faces than larger faces, where confidence levels from larger detection windows are used to drive the increments for smaller detection windows, the savings made possible by embodiments of the present invention are greater than if smaller detection windows were applied first.

In the embodiments described above, for a given detection window size, either a large or small x or y increment is employed depending on whether or not a face is likely to be in the vicinity of a detection window location. However, the increment can be varied in any suitable way. So for example, the increment could be made inversely proportional to the confidence level of previous detection windows applied in the region.

Alternatively, instead of returning a quasi-continuous value as described above, the confidence level returned by the face detection process 34 could be discretely-valued indicating either: (i) no face; (ii) possible face; or (iii) face, each causing the advance step 40 to act as set out in relation to Figure 4.

The detection window does not have to move along a row. Instead, its progress in each of the x and y directions may be adjusted from one increment to the next as a function of the confidence level of previous detection windows applied in the region.

The embodiments described above can be implemented in a digital image processing device such a digital stills camera, a digital video camera, camera phone or the like. The embodiments due to their computational efficiency can be implemented within a real-time face detection function which for example enables the device to highlight with a respective boundary (corresponding to a detection window) in a viewfinder faces detected in an acquired image or image stream.

Alternatively or in addition, the embodiments can be implemented within an off-line face detection function either within a digital image processing device or in a connected computing device to which an image is transferred or which has access to the image, to provide more efficient face detection.

Alternatively or in addition, the detected face regions can be employed with image post-processing functions such as red-eye detection and/or correction, or for example face expression detection and/or correction, or face recognition.

Where the detected face regions are employed in facial recognition, as many facial recognition systems remain sensitive to slight variations in either facial rotation or size, it is advantageous to apply post-processing measures in order to optimize the accuracy of facial recognition. This is because, even where frontal face regions are detected and saved, these regions may not be optimally aligned or scaled for the purposes of face recognition. Also, it should be noted that many images captured are consumer images and that subjects in such images will rarely maintain their faces in a squarely facing frontal position at the time of image acquisition.

Where as in the embodiment above, the face detection employed is highly optimized for speed and for the accurate determination of the presence of a face region, face detection is typically not optimized to accurately match the precise scale, rotation or pose of a detected face region.

There are many techniques known in the prior art for achieving such normalization, however, in an embedded imaging device, such as a digital camera, where processing must be both compact in terms of code footprint and efficient resource usage, it can be impractical to deploy more of such complex processing.

Thus, in one embodiment the face detector, already available within the image acquisition device, can be re-purposed for use in post-processing of detected/tracked face regions. In the embodiment, a supplementary *frontal face* detector which is generally identical to a standard detector, but highly optimized at the training stage to detect only

frontal faces is employed. So for example, the frontal face detector would not be suitable for normal face detection/tracking where a more relaxed detector, hereafter referred to as a *standard* detector is required.

Referring now to Figure 5, in this embodiment, if a face region to which face recognition is to be applied is originally detected, step 50, with an initial probability less than a 1st threshold, the region is expanded by say, X=20% to include a surrounding peripheral region and extracted from the acquired image, step 52. This larger region is typically sufficient to contain the entire face.

A standard detector is next applied to the expanded region, step 54, but across a smaller range of maximum and minimum scales, and at finer granular resolution than would be employed across a full image.

As an example, at step 54, the detector might scale from 1.1 to 0.9 times the size of the face region determined by the original detection process, step 50, but in increments of 0.025; thus 0.9, 0.925, 0.95, 0.975, 1.00, and so on, and similarly with step size. The goal is to determine a sub-window optimized in scale and alignment within the extracted, expanded face region where the face probability is highest. Ideally, such a sub-window will exceed a 2nd threshold probability for face detection no less than the 1st threshold. If not, and if rotation is not to be applied in an attempt to improved this probability, then this face region is marked as "unreliable" for recognition, step 56.

Where the first or second thresholds are exceeded then either the sub-window for the originally detected face region or the optimized window from step 54 are expanded by say Y = 10% < X, step 58.

The *frontal face* detector is then applied to the expanded region, step 60. If a sub-window with a face detection probability above a third threshold (higher than each of the first and second thresholds is identified), step 62, then that sub-window is marked as "reliable" and is passed on to a recognition process, step 64.

Where the *frontal face* detection step fails at step 62, but we know there is a high probability face region, then it is likely that one or both of a small rotational or pose normalization is also required to produce a face region suitable for face recognition.

In one embodiment, the original X% expanded face region is next rotated through one of a number of angular displacements, say -0.2, -0.15, -0.1, -0.05, 0.0, +0.05, +0.1, +0.15 and +0.2 radians, step 66, and the fine grained standard face detection and possibly frontal face detection steps are re-applied as before.

Ideally, the face probability will increase above the required 3rd threshold as these angular rotations are applied to the extracted face region and the face region can be marked as "reliable". It will also be seen that the potentially changing probabilities from face region rotation can also be used to guide the direction of rotation of the region. For example, if a rotation of -0.05 radians increases the face detection probability but not sufficiently, then the next rotation chosen would be -0.1 radians. Whereas if a rotation of -0.05 radians decreases the face detection probability, then the next rotation chosen would be 0.05 radians and if this did not increase the face detection probability, then the face region could be marked as "unreliable" for recognition, step 56

As an alternative or in addition to this in-plane rotation of the face region, an AAM (Active Appearance Model) or equivalent module can be applied to the detected face region in an attempt to provide the required pose normalization to make the face region suitable for face recognition. AAM modules are well known and a suitable module for the present embodiment is disclosed in "Fast and Reliable Active Appearance Model Search for 3-D Face Tracking", F Dornaika and J Ahlberg, IEEE Transactions on Systems, Man, and Cybernetics-Part B: Cybernetics, Vol 34, No. 4, pg 1838-1853, August 2004, although other models based on the original paper by TF Cootes et al "Active Appearance Models" Proc. European Conf. Computer Vision, 1998, pp 484-498 could also be employed.

In this embodiment, the AAM model has two parameters trained for horizontal and vertical pose adjustments, and the AAM model should converge to the face within the detected face region indicating the approximate horizontal and vertical pose of the face. The face region may then be adjusted by superimposing the equivalent AAM model to provide a "straightened" face region rotated out of the plane of the image, step 68.

Again, fine grained standard face detection and frontal face detection steps are re-applied, and if the threshold for the detected face region(s) is not above the required probability, then small incremental adjustments of the horizontal and vertical pose may be stepped through as before until either the *frontal face* detector probability increases sufficiently to mark the face region as "reliable" or the face region is confirmed to be "unreliable" to use for face recognition purposes.

US Patent Application 11/752,925 filed May 24, 2007 (Ref: FN172) describes capturing face regions from a preview stream and subsequently aligning and combining these images using super-resolution techniques in order to provide a repair template for portions of a facial region in a main acquired image. These techniques may be advantageously employed,

in addition to or as an alternative to the steps above, independently or as part of a post-processing step on a face region in order to bring the face region into a substantially frontal alignment before face recognition.

In other alternative applications for detected face regions, the selected regions may be consecutively applied to a series of images such as preview images, post-view images or a video stream of full- or reduced-resolution images, or combinations thereof, where the confidence level as well as the window locations are passed from one preview image, post-view image, etc., to the next.

While an exemplary drawings and specific embodiments of the present invention have been described and illustrated, it is to be understood that that the scope of the present invention is not to be limited to the particular embodiments discussed.

In addition, in methods that may be performed according to preferred embodiments herein and that may have been described above, the operations have been described in selected typographical sequences. However, the sequences have been selected and so ordered for typographical convenience and are not intended to imply any particular order for performing the operations, except for those where a particular order may be expressly set forth or where those of ordinary skill in the art may deem a particular order to be necessary.

Claims:

1. A method of detecting a face in an image comprising:

(a) performing face detection within a first window of said image at a first location;

(b) obtaining from said face detection a confidence level indicating a probability of said image including a face at or in the vicinity of said first location; and

(c) performing said face detection within a second window at a second location wherein said second location is determined based on said confidence level.

2. A method as claimed in claim 1, wherein direction and magnitude of displacement within said image from said first location to said second location comprise a function of said confidence level.

3. A method as claimed in claim 1, further comprising repeating (a) to (c) for one or more additional windows in different locations until said performing face detection results in positive detection of a face.

4. A method as claimed in claim 1 further comprising repeating (a) to (c) for one or more additional windows in different locations until face detection has been performed over an entire region of interest.

5. A method as claimed in claim 4, wherein the dimensions of said one or more additional windows depend on said confidence level.

6. A method as claimed in claim 1, further comprising repeating (a) to (c) until face detection for multiple predetermined sizes of windows has been performed over an entire region of interest of said image.

7. A method as claimed in claim 1, further comprising

determining a set of regions of interest for said image, and

repeating steps (a) to (c) for all said regions of interest.

8. A method as claimed in claim 1, further comprising identifying at least one region of said image likely to contain a face; and repeating (a) to (c) until face detection is performed over substantially an entirety of said at least one region.

9. A method as claimed in claim 1, further comprising identifying at least one region of said image likely to contain a face; and repeating (a) to (c) until face detection is performed concentrically inside said at least one region.

10. A method as claimed in claim 1, wherein said face detection comprises applying a chain of classifiers to said windows of said image and wherein said confidence level comprises a function of a number of classifiers successfully applied to said windows.

11. A method as claimed in 1, wherein said face detection returns a confidence level indicating that no face is present in the vicinity of said first location, that a face may be present in the vicinity of said first location, or that a face is present at said first location.

12. A method as claimed in claim 1, wherein said second location is determined by advancing said window in an x-amount in a first direction and in an orthogonal second direction by y-amount from the first location, wherein any overlap of the first and second windows is based on a said confidence level.

13. A method as claimed in claim 12, wherein a size of the second window relative to a size of said first window is also based on said confidence level.

14. A method as in claim 12, wherein the x-amount or y-amount, or both, are less for a higher confidence level that the image includes a face in the vicinity of the first location.

15. A method as claimed in claim 12, wherein the x-amount or the y-amount, or both, are greater for a higher confidence level that the image includes a face at the first location.

16. A method as claimed in claim 12, wherein the x-amount or the y-amount, or both, are greater for a higher confidence level that the image does not include a face at the first location.

17. A method as claimed in claim 12, wherein the x-amount and the y-amount depend separately on face detection confidence levels in the first and second directions, respectively.

18. A method as claimed in claim 1, wherein when there is a confidence level above a threshold value that a face is detected in the vicinity of said first location, then the second location is selected such that the second window overlaps said first window to center on said face, and when there is a confidence level below said threshold, the second location is selected so that the second window does not overlap the first window.

19. A method as claimed in claim 1, further comprising pre-determining one or more regions of interest within the image each as having an enhanced likelihood of including a face, and locating a detection window at a suitable corner of each such region of interest, and applying (a) to (c) to each such region of interest.

20. A method as claimed in claim 19, wherein (a) to (c) are applied to two or more regions of interest in time periods with at least some temporal overlap.

21. A method as claimed in claim 19, wherein said one or more regions of interest comprise one or more regions including a number of skin pixels.

22. A method as claimed in claim 19, wherein said image is an image in a stream of images and wherein said regions of interest comprise one or more regions in which a face has been detected in a previous image of said stream.

23. A method as claimed in claim 1 wherein said step (c) comprises:

responsive to said confidence level indicating a face at or in the vicinity of said first location, performing detection of a frontally aligned face within a second window at a second

location wherein said second location is determined based on a confidence level indicating a probability of a candidate region including said face at or in the vicinity of said first location.

24. A method as claimed in claim 23 comprising:

(d) responsive to detection of a frontally aligned face in any candidate region, selectively applying face recognition to said candidate region.

25. A method as claimed in claim 24 wherein face recognition is applied in response to any candidate region having a probability of including a face greater than a threshold.

26. A method as claimed in claim 23 wherein said performing detection of a frontally aligned face is performed in a candidate region including said face detected at or in the vicinity of said first location.

27. A method as claimed in claim 26 wherein performing detection of a frontally aligned face is performed in response to said candidate region having a probability of including a face greater than a first threshold.

28. A method as claimed in claim 26 comprising:

responsive to said first location having a probability of including a face less than a first threshold, extracting an extended region including said first location from said image and performing face detection in said extended region with a relatively fine granularity to provide said candidate region.

29. A method as claimed in claim 26 comprising:

responsive to a candidate region having a probability of including a face less than a second threshold, rotating an extended region including said face region through one of a sequence of angles and performing face detection in said rotated extended region with a relatively fine granularity to provide another candidate region.

30. A method as claimed in claim 26 comprising:

responsive to a candidate region having a probability of including a face less than a second threshold, rotating said face within said extended region through one of a sequence of

angles and performing face detection in said extended region with a relatively fine granularity to provide another candidate region.

31. A digital image processing device adapted to:

(a) perform face detection within a first window of an acquired image at a first location;

(b) obtain from said face detection a confidence level indicating a probability of said image including a face at or in the vicinity of said first location; and

(c) perform said face detection within a second window at a second location wherein said second location is determined based on said confidence level.

32. A computer program product which when executed in a digital image processing device is operable to perform the steps of:

(a) performing face detection within a first window of an acquired image at a first location;

(b) obtaining from said face detection a confidence level indicating a probability of said image including a face at or in the vicinity of said first location; and

(c) performing said face detection within a second window at a second location wherein said second location is determined based on said confidence level.

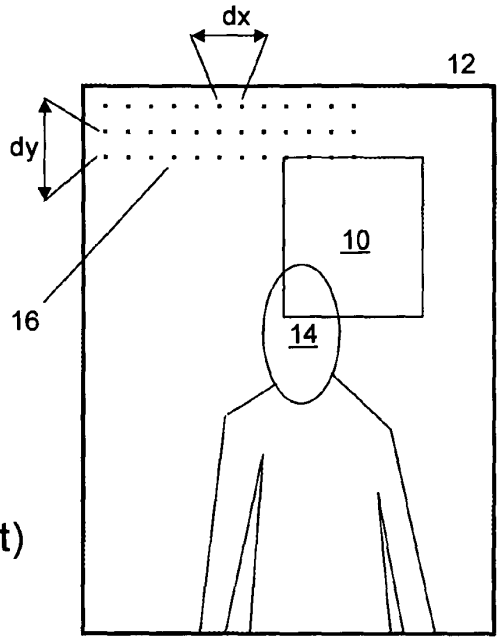


Figure 1
(Prior art)

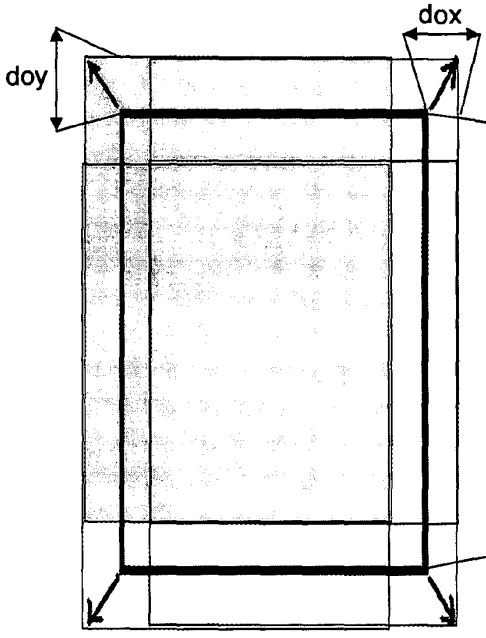


Figure 2(a)

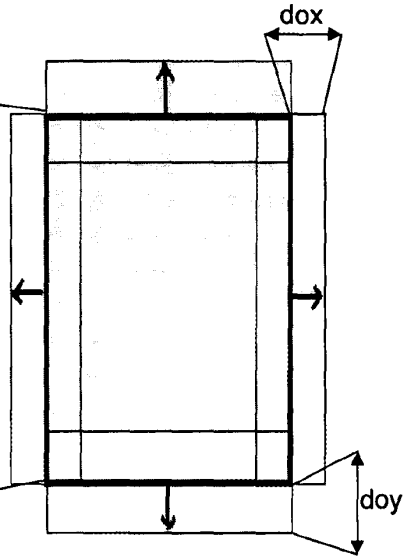


Figure 2(b)

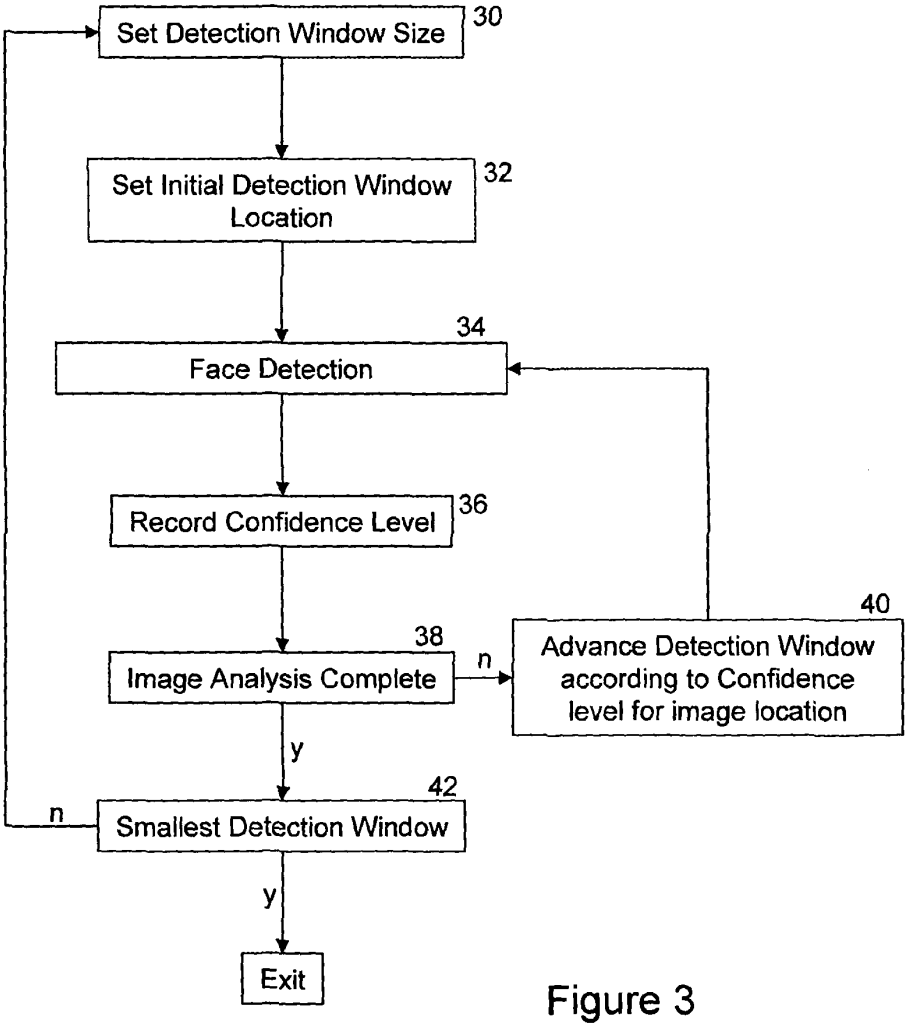

Set Detection Window Size
30
Set Initial Detection Window Location
32
34
Face Detection
Record Confidence Level
36
40
38
Image Analysis Complete
n
Advance Detection Window according to Confidence level for image location
y
42
n
Smallest Detection Window
y
Exit

Figure 3

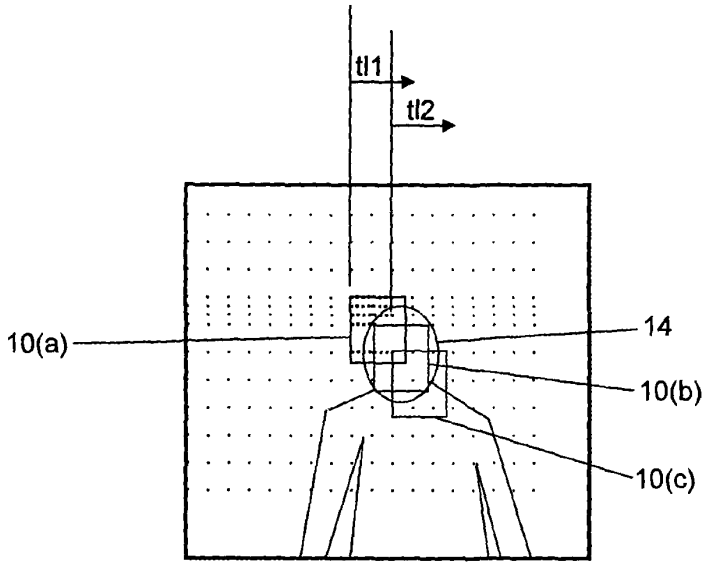


Figure 4

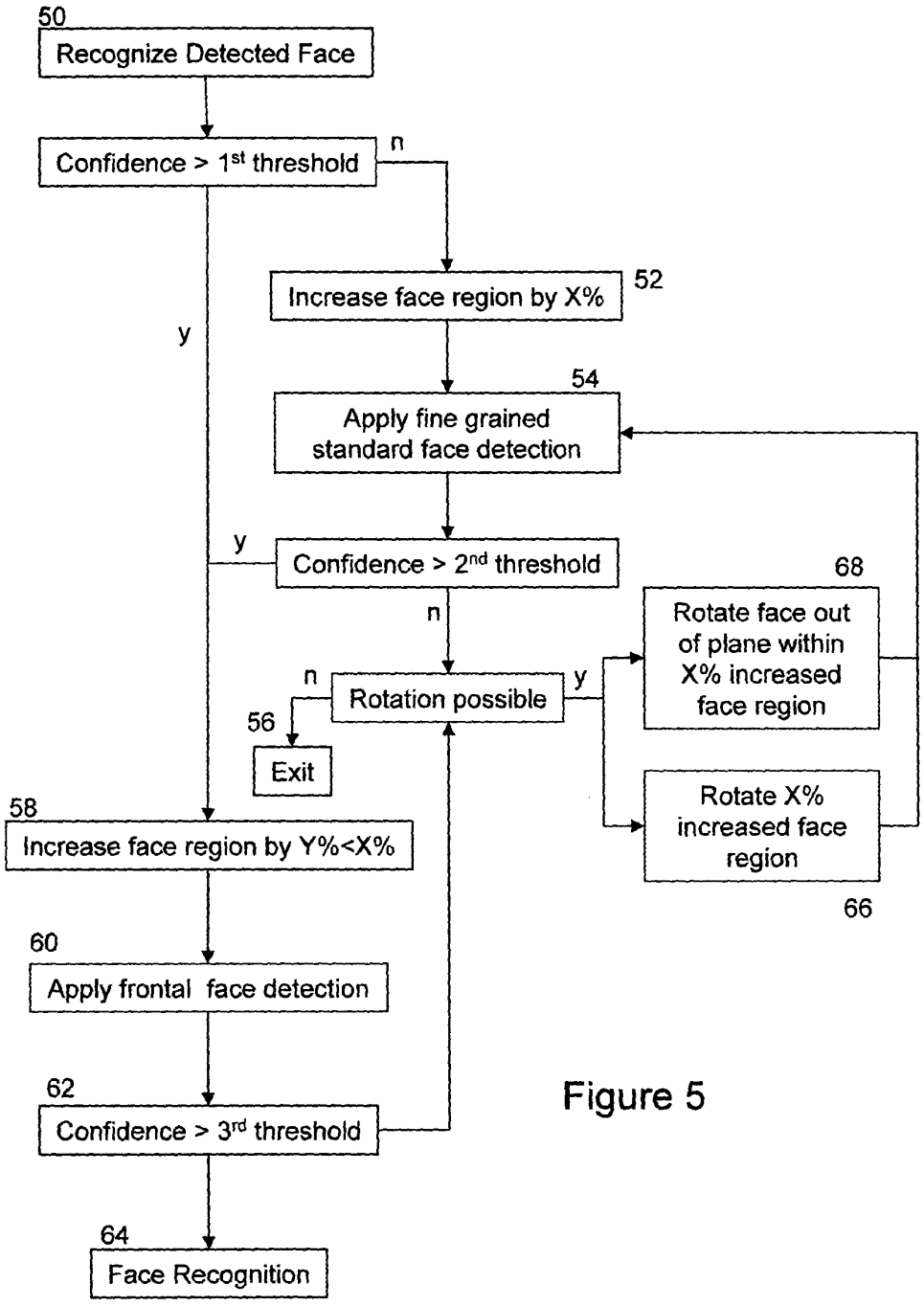

50
Recognize Detected Face
Confidence > 1st threshold
n
Increase face region by X%
52
y
54
Apply fine grained standard face detection
y
Confidence > 2nd threshold
68
n
Rotate face out of plane within X% increased face region
n
Rotation possible
y
56
Exit
58
Increase face region by Y%<X%
Rotate X% increased face region
66
60
Apply frontal face detection
62
Confidence > 3rd threshold
64
Face Recognition

Figure 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2007/006540

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06K9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/264744 A1 (ZHANG LEI [CN] ET AL) 30 December 2004 (2004-12-30) abstract; figures 3-6 paragraphs [0005], [0061] - [0071], [0076] - [0078], [0082] - [0087]	1-16, 18-27, 31,32
X	HENRY A. ROWLEY: "Neural Network-Based Face Detection" May 1999 (1999-05), CARNEGIE MELON UNIVERSITY , PITTSBURG, PA, USA , XP002456221 Chapter 6 page 92 subsection 8.3	1-9,11, 19-32

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 October 2007	08/11/2007

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Alecu, Teodor Iulian

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	HANJIN RYU ET AL: "Coarse-to-Fine Classification for Image-Based Face Detection" IMAGE AND VIDEO RETRIEVAL LECTURE NOTES IN COMPUTER SCIENCE;;LNCS, SPRINGER-VERLAG, BE, vol. 4071, July 2006 (2006-07), pages 291-299, XP019036040 ISBN: 3-540-36018-2 Sections 1 and 3	1-4, 6-28,31, 32
X	EP 1 626 569 A (FUJI PHOTO FILM CO LTD [JP]) 15 February 2006 (2006-02-15) paragraphs [0077], [0087] - [0099], [0107] - [0111], [0121] - [0124], [0161]	1-9, 11-16, 18,19, 21,23-32
X	MEKUZ, N. AND DERPANIS, K.G. AND TSOTSOS, J.K.: "ADAPTIVE STEP SIZE WINDOW MATCHING FOR DETECTION" PROCEEDINGS OF THE 18TH INTERNATIONAL CONFERENCE ON PATTERN RECOGNITION, vol. 2, August 2006 (2006-08), pages 259-262, XP002455696 Hong Kong, China Sections 1 and 2	1-6, 11-18, 23-27, 31,32
X	SMERALDI F ET AL: "Facial feature detection by saccadic exploration of the Gabor decomposition" IMAGE PROCESSING, 1998. ICIP 98. PROCEEDINGS. 1998 INTERNATIONAL CONFERENCE ON CHICAGO, IL, USA 4-7 OCT. 1998, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, vol. 3, 4 October 1998 (1998-10-04), pages 163-167, XP010586874 ISBN: 0-8186-8821-1 Sections 4 to 6 Sub-section 7.2	1-4,11, 12, 14-16, 18-20, 22-28, 31,32
X	FROBA, B., ERNST, A. AND KUBLBECK, C.: "Real time face detection" PROCEEDINGS OF IASTED "SIGNAL AND IMAGE PROCESSING", [Online] 2002, pages 1-6, XP002455698 Kauai, Hawai Retrieved from the Internet: URL:http://www.embassi.de/publi/veroeffent /Froeba.pdf> [retrieved on 2007-10-23] Sections 1,2,6	1-4, 6-11,19, 21,23-32

-/--

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	FERAUD R ET AL: "A FAST AND ACCURATE FACE DETECTOR BASED ON NEURAL NETWORKS" IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, IEEE SERVICE CENTER, LOS ALAMITOS, CA, US, vol. 23, no. 1, 1 January 2001 (2001-01-01), pages 42-53, XP001008995 ISSN: 0162-8828 Section 2; subsection 2.1 Section 3	1-4,6-9, 11, 19-28, 31,32
A	FROBA, B. AND ERNST, A.: "Face detection with the modified census transform" PROCEEDINGS OF THE SIXTH IEEE INTERNATIONAL CONFERENCE ON AUTOMATIC FACE AND GESTURE RECOGNITION, 2004, pages 91-96, XP002455697 cited in the application the whole document	1-32
A	US 2006/029265 A1 (KIM JUNGBAE [KR] ET AL) 9 February 2006 (2006-02-09) abstract; figures 1,8 paragraphs [0029] - [0055]	1-32

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2007/006540

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004264744 A1	30-12-2004	NONE	
EP 1626569 A	15-02-2006	JP 2006285944 A	19-10-2006
		US 2006035259 A1	16-02-2006
US 2006029265 A1	09-02-2006	KR 20060012777 A	09-02-2006

Form PCT/ISA/210 (patent family annex) (April 2005)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 May 2015 (21.05.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/070320 A1

(51) International Patent Classification:
G06K 9/46 (2006.01) *G06T 3/60* (2006.01)
G06K 9/62 (2006.01) *G06T 5/00* (2006.01)
G06Q 30/02 (2012.01)

(21) International Application Number:
PCT/CA2014/000802

(22) International Filing Date:
12 November 2014 (12.11.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14/078,071 12 November 2013 (12.11.2013) US

(71) Applicant: **APPLIED RECOGNITION INC.** [CA/CA]; 3307 Lakeland Crescent, Burlington, Ontario L7N 1B9 (CA).

(72) Inventors: **GANONG, Ray**; 3307 Lakeland Crescent, Burlington, Ontario L7N 1B9 (CA). **WAUGH, Donald, Craig**; 332 Creek Path Avenue, Oakville, Ontario L6L 6X1 (CA). **MAN RO, Wang**; Miseong Apt. 22-1101, Apgujeong-Dong, Gangnam-Gu, Seoul 135-785 (KR). **PLATANIOTIS, Konstantinos**; 24 Wellesley Street West, Toronto, Ontario M4Y 2X6 (CA). **STUDHOLME, Chris**; 104 Esterlawn Private, Ottawa, Ontario K2A 4B5 (CA).

(74) Agent: **NORTON ROSE FULBRIGHT CANADA LLP**; 1 Place Ville Marie, Suite 2500, Montreal, Quebec H3B 1R1 (CA).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU,

[Continued on next page]

(54) Title: FACE DETECTION AND RECOGNITION

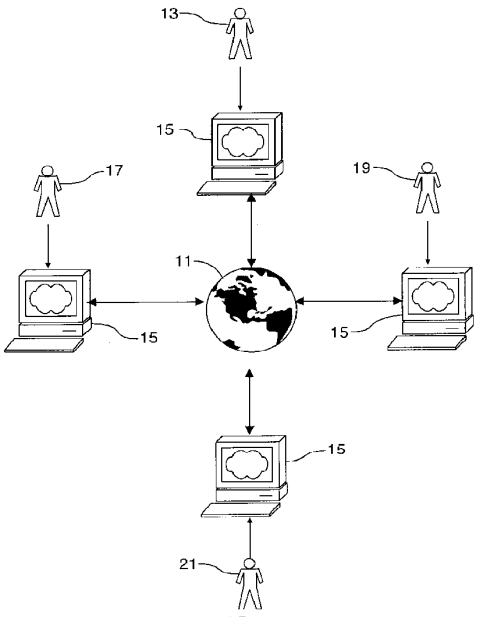


FIG.1

(57) Abstract: The present invention provides, in at least one aspect, methods and systems that detect at least one face in at least one digital image, determine and store area co-ordinates of a location of the at least one detected face in the at least one digital image, apply at least one transformation to the at least one detected face to create at least one portrait of the at least one detected face, rotate the at least one portrait at least until the at least one portrait is shown in a vertical orientation and a pair of eyes of the at least one face shown in the at least one portrait are positioned on a horizontal plane; and store the rotated at least one portrait.

WO 2015/070320 A1

LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

FACE DETECTION AND RECOGNITION

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority from U.S. patent application serial no. 14/078,071, filed November 12, 2013 entitled "FACE DETECTION AND RECOGNITION", of which the entire contents is hereby incorporated by reference in its entirety.

FIELD OF THE INVENTION

[0002] The present invention relates to face and portrait extraction using face detection and recognition and application thereof.

BACKGROUND OF THE INVENTION

[0003] Social networks presently exist as a means to connect individuals using a website. The following definition exists in the PCMAG.COM™ encyclopedia for "social network":

> [0004] An association of people drawn together by family, work or hobby. The term was first coined by Professor J. A. Barnes in the 1950s, who defined the size of a social network as a group of about 100 to 150 people.

[0005] The following definition exists in the PCMAG.COM™ encyclopedia for "social network site":

> [0006] A Web site that provides a virtual community for people interested in a particular subject or just to "hang out" together. Members communicate by voice, chat, instant message, videoconference and blogs, and the service typically provides a way for members to contact friends of other members. Such sites may also serve as a vehicle for meeting in person. The "social networking site" is the 21st century term for "virtual community," a group of people who use the Internet to communicate with each other about anything and everything.
>
> [0007] Friendster (www.friendster.com) was the first social networking site, which was introduced in 2002 and followed by MySpace (www.myspace.com) a year later. Started by two friends, MySpace became extremely popular, and its parent company, Intermix, was acquired by News Corporation for $580 million two years after MySpace was launched.

[0008] Facebook (www.facebook.com) came out in 2004 initially targeting college students, but later welcoming everyone. Following Facebook were TagWorld (www.tagworld.com) and Tagged (www.tagged.com). TagWorld introduced tools for creating more personalized Web pages, and Tagged introduced the concept of building tag teams for teens with like interests.

[0009] Social networking sites compete for attention much like the first Web portals when the Internet exploded onto the scene in the mid-1990s. Many variations are expected.

[0010] Many social network sites allow users to upload and share photos. Some also incorporate a feature for tagging photos to identify the names of people (faces) in the photos (FACEBOOK™, for example, provides this feature). Based on user surveys the majority of respondents state that the tagging effort is manual and very time consuming. Also, for privacy reasons, many users do not upload all of their digital photos to the sharing website. It is also very time consuming and bandwidth intensive to upload thousands of photos. So while a user of a social network site may have 10,000 digital photos on their local computer, they only upload one or two hundred to share with their friends. This is based on user surveys conducted by Applied Recognition Inc. in September 2007.

[0011] There are also websites that allow registered users to upload digital photos and digital video and store them on a website for sharing purposes. These are dedicated to this purpose. Examples of these sites include FLICKR™ and PHOTOBUCKET™. The drawback with these sites is that all tagging of photos to identify friends is manual and time consuming; PHOTOBUCKET™ does not allow people tagging in a photo. With FLICKR™, if an average photo contains two people, then it may take 10 – 15 seconds per photo to tag the people. When that time is multiplied by 100 or 1000, it becomes too time-consuming and the average person just will not perform tagging.

[0012] Rapid growth in photo-taking devices is occurring today with the incorporation of digital cameras in most modern cell phones. In fact, more cameras are sold via cell phones today than all dedicated digital cameras combined. This is causing a proliferation in the number of digital images that are uploaded and stored on home computers. Because the average number of digital images exceeds 1000 based on our surveys, the effort is too great to manually tag and properly organize the images for the majority of people.

[0013] One company, RIYA™ (www.riya.com), created a product that is web-based for identifying faces in digital photos. This product involved the download of a software module for identifying faces in photos on the user's local computer before uploading these photos to the remote RIYA™ web-based server where the faces were compared with other faces to find matches. This product is a prototype and as such has no automatic photo sharing features based on recognition. It also has no features for enabling the user to correct the inevitable errors that occur in any automated face detection and recognition method.

[0014] Prior to 2007, image searches were conducted using text or dates related to the photo such as captions, titles, description, creation date, etc., as opposed to the image content itself. Since then there have been a number of companies that began introducing face detection and recognition in consumer photo applications including: in 2008, Google introduced face recognition into Picasa; Polar Rose application for Flickr in 2009; Apple purchased Polar Rose in 2010 and introduced the feature in iPhoto; Microsoft introduced face recognition their Photo Gallery product in 2010; Facebook introduced face detection in 2010; and in 2010 Sony Ericsson integrated face-recognition software into its photo gallery.

SUMMARY OF THE INVENTION

[0015] In one aspect of the present invention, a method for recognizing one or more faces in a digital image is provided, the method characterized by: (a) generating one or more face coordinates corresponding to one or more candidate regions for one or more faces; (b) generating eye coordinates based on the face coordinates; (c) detecting each face using one or more projection images defined by the face coordinates and the eye coordinates; and (d) comparing each projection image with one or more known projection images, wherein a similarity threshold is provided for defining a best match between the projection image and the known projection images.

[0016] In another aspect of the present invention, a method for sharing a digital image depicting one or more faces is provided, the method characterized by: (a) linking a plurality of computer terminals to a computer network, each computer terminal associated with an individual; (b) linking the digital image to at least one of the computer terminals; (c) enabling at least one of the computer terminals to initiate a face recognition routine on the digital image, the face recognition routine producing a list of one or more persons whose faces are depicted in the digital image, at least one of the persons being one of the individuals; and (d) enabling at least

one of the computer terminals to initiate a sharing routine for disseminating the digital image to the computer terminals associated with the one or more persons.

[0017] In another aspect of the present invention, a method for sharing a digital image depicting one or more faces is provided, the method characterized by: (a) linking a plurality of computer terminals to a computer network and a plurality of cloud services with the digital images and metadata stored in a cloud-based data repository. (b) linking the digital image to at least one of the computer terminals; (c) enabling at least one of the computer terminals to initiate a face recognition routine on the digital image, the face recognition routine producing a list of one or more persons whose faces are depicted in the digital image, at least one of the persons being one of the individuals; and (d) enabling at least one of the computer terminals to initiate a sharing routine for disseminating the digital image to the computer terminals associated with the one or more persons.

[0018] In another aspect of the present invention, a method for sharing a digital image depicting one or more faces is provided, the method characterized by: (a) linking a plurality of computer terminals to a computer network, each computer terminal associated with an individual and a plurality of cloud services with the digital images and metadata stored on each computer terminal and in a cloud-based data repository. (b) linking the digital image to at least one of the computer terminals; (c) enabling at least one of the computer terminals to initiate a face recognition routine on the digital image, the face recognition routine producing a list of one or more persons whose faces are depicted in the digital image, at least one of the persons being one of the individuals; and (d) enabling at least one of the computer terminals to initiate a sharing routine for disseminating the digital image to the computer terminals associated with the one or more persons.

[0019] In another aspect of the present invention, a method for sharing a digital image depicting one or more faces is provided, the method characterized by: (a) linking a plurality of a cameras or smart phones with cameras taking a picture or taking video images and linking a plurality of computer terminals to a computer network, each computer terminal associated with an individual and a plurality of cloud services with the digital images and metadata stored on each computer terminal and in a cloud-based data repository. (b) linking the digital image to at least one of the computer terminals; (c) enabling the cameras or smart phones with cameras to initiate a face recognition routine on the digital image, the face recognition routine producing a list of one or more persons whose faces are depicted in the digital image, at least one of the persons being one of the individuals; and (d) enabling at least one of the computer terminals to

initiate a sharing routine for disseminating the digital image to the computer terminals associated with the one or more persons.

[0020] In a further aspect of the present invention, a system for recognizing one or more faces in a digital image is provided, the system characterized by: (a) one or more face coordinates corresponding to one or more candidate regions for one or more faces; (b) eye coordinates generated based on the face coordinates; (c) one or more projection images defined by the face coordinates and the eye coordinates; and (d) a similarity threshold for defining a best match between each projection image and one or more known projection images, the best match determining an identity corresponding to each of the one or more faces.

[0021] In a still further aspect of the present invention, a system for sharing a digital image depicting one or more faces is provided, the system characterized by: (a) a plurality of computer terminals linked to a computer network, each computer terminal associated with an individual; (b) a digital image operable to be linked to at least one of the computer terminals; (c) a face recognition routine operable to be initiated by at least one of the computer terminals, the face recognition routine producing a list of one or more persons whose faces are depicted in the digital image, at least one of the persons being one of the individuals; and (d) a sharing routine operable to be initiated by at least one of the computer terminals, the sharing routine disseminating the digital image to the computer terminals associated with the one or more persons.

[0022] In yet another aspect of the present invention, a method for providing secure targeted advertising is provided, the method characterized by: (a) tracking one or more demographic properties associated with an individual registered to a computer program; (b) retrieving from a first source a list of advertising pointers associated with one or more advertisements targeted based on the one or more demographic properties; (c) retrieving from a second source the one or more advertisements; (d) deleting the one or more demographic properties from the first source; and (e) presenting the advertisements to the individual.

[0023] In a further aspect of the present invention, a system for recognizing one or more faces in a digital image is provided, the system characterized by: (a) one or more face coordinates corresponding to one or more candidate regions for one or more faces; (b) eye coordinates generated based on the face coordinates; (c) one or more projection images defined by the face coordinates and the eye coordinates; and (d) a similarity threshold for defining a best match between each projection image and one or more known projection images, the best match determining an identity corresponding to each of the one or more faces.

[0024] In a still further aspect of the present invention, a system for sharing a digital image depicting one or more faces is provided, the system characterized by: (a) a plurality of computer terminals linked to a computer network, each computer terminal associated with an individual; (b) a digital image operable to be linked to at least one of the computer terminals; (c) a face recognition routine operable to be initiated by at least one of the computer terminals, the face recognition routine producing a list of one or more persons whose faces are depicted in the digital image, at least one of the persons being one of the individuals; and (d) a sharing routine operable to be initiated by at least one of the computer terminals, the sharing routine disseminating the digital image to the computer terminals associated with the one or more persons.

[0025] In yet a further aspect of the present invention, a system for providing secure targeted advertising is provided, the system characterized by: (a) one or more demographic properties associated with an individual registered to a computer program; (b) a first source operable to provide a list of advertising pointers associated with one or more advertisements targeted based on the one or more demographic properties; (c) a second source operable to provide the one or more advertisements; (d) a means for deleting the one or more demographic properties from the first source; and (e) a means for presenting the advertisements to the individual.

[0026] In a further still aspect of the present invention, a computer program product for recognizing one or more faces in a digital image is provided, the computer program product characterized by: (a) a computer readable medium including software instructions; and (b) the software instructions for enabling the computer to perform predetermined operations, the predetermined operations including the steps of: (i) generating one or more face coordinates corresponding to one or more candidate regions for one or more faces; (ii) generating eye coordinates based on the face coordinates; (iii) detecting each face using one or more projection images defined by the face coordinates and the eye coordinates; and (iv) comparing each projection image with one or more known projection images, wherein a similarity threshold is provided for defining a best match between the projection image and the known projection images.

[0027] In another aspect of the present invention, a computer program product for sharing a digital image depicting one or more faces is provided, the computer program product characterized by: (a) a computer readable medium including software instructions; and (b) the software instructions for enabling the computer to perform predetermined operations, the

predetermined operations including the steps of: (i) linking a plurality of computer terminals to a computer network, each computer terminal associated with an individual; (ii) linking the digital image to at least one of the computer terminals; (iii) enabling at least one of the computer terminals to initiate a face recognition routine on the digital image, the face recognition routine producing a list of one or more persons whose faces are depicted in the digital image, at least one of the persons being one of the individuals; and (iv) enabling at least one of the computer terminals to initiate a sharing routine for disseminating the digital image to the computer terminals associated with the one or more persons.

[0028] In yet another aspect of the present invention, a computer program product for providing secure targeted advertising is provided, the computer program product characterized by: (a) a computer readable medium including software instructions; and (b) the software instructions for enabling the computer to perform predetermined operations, the predetermined operations including the steps of: (i) tracking one or more demographic properties associated with an individual registered to a computer program; (ii) retrieving from a first source a list of advertising pointers associated with one or more advertisements targeted based on the one or more demographic properties; (iii) retrieving from a second source the one or more advertisements; (iv) deleting the one or more demographic properties from the first source; and (v) presenting the advertisements to the individual.

[0029] The present invention, in a further aspect thereof, enables capturing portraits of people whose faces are located in an image. If faces are detected in an image, the computer program herein provided captures the XY coordinates of the location of the face and records this in the database. The computer program may be configured to adjust the size of the face region in order to capture and create a portrait (or thumbnail) of the person. Furthermore the computer program provided herein may automatically adjust the rotation of the face to render the face position vertically for the portrait with eyes on a horizontal plane.

[0030] The present invention, in a further aspect thereof, enables the utilization of portraits captured and stored in a database of people whose faces are located in an image. The computer program may select and merge a portrait with an advertisement or a product image for display to the consumer. The computer program may be configured to adjust the size of the portrait to match the size requirements of the advertisement or product image

[0031] The present invention, in a further aspect thereof, enables hiding of people whose faces are located in an image. The computer program queries the database for the XY coordinates of the location of the face to be suppressed. The user of the computer program may

select an image that is used to mask the existing face region. The computer program will overlay the selected image over the face of the selected person - in a single image or all images containing that person - and display the modified image to the consumer. This action may be taken for entertainment purposes or to hide negative memories. The computer program may be configured to adjust the size of the portrait to match the size requirements of the selected face size to hide. The computer program may store the modifications in metadata or apply the changes permanently to the original photo. The edges of the overlayed (replacement) image may be adjusted to match color, intensity, brightness, texture and other characteristics to blend into the original image and be more visually appealing.

[0032] Yet another aspect of the present invention enables the display of faces or portraits captured from photos in historical order. The computer program enables the capturing of portraits from images. The computer also tracks the date of the photo either from file information, EXIF (metadata) information or the user of the computer program may optionally specify a date for an image such as is required for scans of older non-digital photos. The computer program employs date data from photos correlated to portraits captured from such photos to arrange the display of the portraits according to date. The computer program can subsequently use photo morphing techniques to generate and display an animation the evolution of a person's face over time.

[0033] Yet another aspect of the present invention enables the faces or portraits captured from photos to be utilized as content for games and exercises. The computer program enables the capturing of portraits from images. The computer program also maintains a database of people in the photos and the relationships between people. The computer program, using such data, correlates the user of the program ("the player") with photos and portraits captured from such photos to arrange the display of said photos and portraits customized based on the player of the game or exercise. Such customization could be a simple as a slide show of the photos based on the relationship. The customization could also be games such as those useful for people with Alzheimer's or Dementia where personal photos and relationships can be presented to the Alzheimer patient as a game or exercise. This category of treatment is generally known as photo reminiscence therapy. The computer program using the index of photos and portraits extracted from photos retrieve such photos and portraits based on database queries and embeds selected images into games and exercises.

[0034] The present invention, in a further aspect thereof, facilitates the creation of a family tree as an index for the photos. The computer program queries the database for all portraits

related to a given user and then presents the same to the user. The user of the computer program then selects the portraits and drags them on to a specific node in the family tree to add a new relationship. The computer program will dynamically spawn additional relationships as the user drags new portraits of relatives on to the family tree diagram. Once all portraits for a given family have been added to the family tree it is complete and then becomes a dynamic index for the consumer to display and locate photos. Optionally the same tree format can be used to connect friends together and show the (self-defined) relationships between different categories of friends. Example would be co-workers, high school friends, college friends, etc.

[0035] The present invention, in a further aspect thereof enables the use of group portraits to act as an index for the photos. This is of particular interest to any organization of people. Typically organizations maintain group photos by year. For example a sports team will have a team photo displaying the players for every season. A scout troop, orchestra, class photo, club etc. will typically use the same approach. The computer program enables the use of group photos and the resultant identification of subjects in said photos to act as an index to photos containing individuals within the group. This enables the organization and structuring of photo displays based on year/season as well as by group members, and group member subsets.

[0036] Yet another aspect of the present invention enables the displays of faces or portraits of missing children, FBI most wanted and similar requirements to find a person. The computer program displays these images to users of the computer program seeking the assistance of users to find the said persons. The computer also delivers the face signatures of the said person being sought and requests the users permission to compare said face signature with their personal database and report potential matches. Should there be a potential match the user will be presented with such potential match and can optionally notify the respective authority of such potential. This could enable the organization to determine a recent or current location of the individual. It could also enable the organization to determine the name of an individual, since the individual's name may be listed in one or more of the user's known persons list.

[0037] In accordance with an aspect of the present invention, there is provided a method performed by at least one computer, the method comprising: detecting at least one face in at least one digital image; determining and storing area co-ordinates of a location of the at least one detected face in the at least one digital image; applying at least one transformation to the at least one detected face to create at least one portrait of the at least one detected face; rotating the at least one portrait at least until the at least one portrait is shown in a vertical orientation

and a pair of eyes of the at least one face shown in the at least one portrait are positioned on a horizontal plane; and storing the rotated at least one portrait.

[0038] In accordance with an aspect of the present invention, there is provided a system comprising at least one computer comprising at least one processor and a non-transitory computer readable memory comprising processing instructions, that when executed by the at least one processor, cause the computer to: detect at least one face in at least one digital image; determine and store area co-ordinates of a location of the at least one detected face in the at least one digital image; apply at least one transformation to the at least one detected face to create at least one portrait of the at least one detected face; rotate the at least one portrait at least until the at least one portrait is shown in a vertical orientation and a pair of eyes of the at least one face shown in the at least one portrait are positioned on a horizontal plane; and store the rotated at least one portrait.

[0039] In accordance with an aspect of the present invention, there is provided a method performed by at least one computer, the at least one computer comprising or interfacing with a database, the database comprising a plurality of portraits, each portrait associated with an identified person shown in the respective portrait, the method comprising: displaying the respective portrait of at least one identified person associated with a user; displaying a visual representation of at least one personal relationship to the user; assigning at least one of the displayed portraits to at least one of the displayed personal relationships, in accordance with a received user input; and storing the personal relationship assignments in the database.

[0040] In accordance with an aspect of the present invention, there is provided a method performed by at least one computer, the at least one computer comprising or interfacing with a database of portraits and digital images, each portrait associated with an identified person shown in the respective portrait, the method comprising: displaying at least one of the digital images; cross-referencing the displayed at least one digital image with the database of portraits to create a list of at least one identified person shown in the at least one digital image; indexing at least a subset of the digital images in accordance with the list of at least one identified person; and in accordance with a user input selecting at least one of the identified persons from the displayed at least one digital image, displaying at least one of the respectively indexed digital images.

[0041] In accordance with an aspect of the present invention, there is provided a method performed by at least one computer, the at least one computer comprising or interfacing with a database of portraits, each portrait associated with an identified person shown in the respective

portrait, the method comprising: receiving at least one unidentified portrait; comparing face signature of the at least one unidentified portrait against face signatures of portraits of identified persons known to the user; in accordance with a positive result of the comparing, prompting the user for confirmation of the positive result; and in accordance with the confirmation, associating the at least one unidentified portrait with the at least one identified person confirmed by the user and storing the at least one unidentified portrait in the database.

[0042] In accordance with an aspect of the present invention, there is provided a method performed by at least one computer, the at least one computer comprising or interfacing with a database of digital images and respective metadata identifying a name of at least one identified person shown in the respective digital image, the method comprising: selecting one of the identified persons from the database; determining a count of a total number of digital images where the identified person appears; for each identified person shown in at least one of the digital images with the selected identified person, determining a count of a total number of digital images where the respective identified person appears with the selected identified person; and displaying a visual representation comprising: a first node representing the selected identified person and the respective count of the total number of digital images where the identified person appears; for each identified person shown in at least one of the digital images with the selected identified person, a second node representing the respective identified person shown in at least one of the digital images with the selected identified person, each respective node further comprising a visual representation of the respective count of the total number of digital images where the respective identified person appears with the selected identified person; and a link between the first node and each second node.

[0043] In accordance with an aspect of the present invention, there is provided a method performed by at least one computer, the at least one computer comprising or interfacing with a database of digital images and respective metadata identifying a name of at least one identified person shown in the respective digital image, the method comprising: selecting one of the identified persons from the database; determining at least one first identified person shown in at least one of the digital images together with the selected identified person; and displaying a visual representation comprising: for each first identified person, a first tier node representing the selected identified person and the respective first identified person being shown in at least one of the digital images together; and for each first identified person, a second tier node representing the respective first identified person being shown in at least one of the digital images without the selected identified person.

[0044] In accordance with an aspect of the present invention, there is provided a method performed by at least one computer, the at least one computer comprising or interfacing with a database of portraits, each portrait associated with an identified person shown in the respective portrait, the method comprising: selecting one of the identified persons from the database; ordering a plurality of the portraits associated with the selected identified person based at least partly on date metadata associated with each respective portrait; displaying a visual representation comprising: a timeline; and an arrangement of the plurality of the portraits along the timeline in accordance with the respective ordering.

[0045] In accordance with an aspect of the present invention, there is provided a method performed by at least one computer comprising or interfacing with a database of digital images and respective metadata identifying a date of the respective digital image, a plurality of the digital images showing at least one respective unidentified person ("unidentified digital images"), the method comprising: sorting the unidentified digital images by the respective date metadata; assigning a respective clustering token to each of the unidentified digital images, wherein the assigning comprises, in accordance with a determination that a subset of the unidentified digital images each show a common unidentified person, assigning a common respective clustering token to each of the unidentified digital images of the subset; grouping the unidentified digital images by respective clustering token; receiving a new digital image and respective metadata identifying a date of the respective new digital image, the new digital image comprising a new unidentified person; performing at least one comparison of the new unidentified person to the at least one respective unidentified person of the plurality of the digital images in an order, wherein for each group of unidentified digital images, performing only a single comparison of the new unidentified person to the respective common unidentified person; and assigning a clustering token to the new digital image in accordance with the comparison performing resulting in a determination of the new unidentified person common to a respective one of the groups of unidentified digital images.

[0046] In accordance with an aspect of the present invention, there is provided a method of suggesting an identification of an unidentified person in a received digital image, the method performed by at least one computer comprising or interfacing with a database of portraits and associated digital images, each portrait associated with an identified person shown in the respective portrait, the method comprising: determining that respective portraits of at least two identified persons shown in one of the digital images satisfy a comparison threshold with a portrait of the unidentified person determined from the received digital image; suggesting an

identification of the unidentified person as the respective one of the at least two identified persons having a respectively associated portrait that is determined to be a closest match to the portrait of the unidentified person from amongst the at least two identified persons; and excluding a remainder of the at least two identified persons from being subsequently suggested from any other one of the digital images as an identification of the unidentified person.

[0047] In accordance with an aspect of the present invention, there is provided a method of suggesting an identification of an unidentified person in a received digital image, the method performed by at least one computer comprising or interfacing with a database of portraits and associated digital images, each portrait associated with an identified person shown in the respective portrait, the method comprising: determining that a respective portrait of at least one identified person shown in at least one of the digital images satisfies a comparison threshold with a portrait of the unidentified person determined from the received digital image; in accordance with the determined at least one of the digital images associated with metadata comprising a date corresponding to date metadata associated with the received digital image, suggesting an identification of the unidentified person as the at least one identified person.

[0048] In accordance with an aspect of the present invention, there is provided a method of suggesting an identification of an unidentified person in a received digital image, the method performed by at least one computer comprising or interfacing with a database of portraits and associated digital images, each portrait associated with an identified person shown in the respective portrait, the method comprising: in accordance with a determination that the received photo comprises at least one identified person associated with a defined group, suggesting an identification of the unidentified person based at least partly on a determination that a respective portrait of at least one identified person associated with the defined group satisfies a comparison threshold with a portrait of the unidentified person determined from the received digital image.

[0049] In accordance with an aspect of the present invention, there is provided a method of suggesting an identification of an unidentified person in a received digital image, the method performed by at least one computer comprising or interfacing with a database of portraits and associated digital images, each portrait associated with an identified person shown in the respective portrait, the method comprising: determining that a respective portrait of at least one identified person shown in at least one of the digital images satisfies a comparison threshold with a portrait of the unidentified person determined from the received digital image; in accordance with the determined at least one of the digital images associated with metadata

comprising: a date corresponding to date metadata associated with the received digital image; and a location within a predetermined distance threshold of location metadata associated with the received digital image; suggesting an identification of the unidentified person as the at least one identified person.

[0050] In accordance with an aspect of the present invention, there is provided a method of suggesting an identification of an unidentified person in a received digital image, the method performed by at least one computer comprising or interfacing with a database of portraits and associated digital images, each portrait associated with an identified person shown in the respective portrait, the method comprising: determining that a respective portrait of at least one identified person shown in at least one of the digital images satisfies a comparison threshold with a portrait of the unidentified person determined from the received digital image; determining that the received digital image is associated with an event, based at least partly on metadata associated with the received digital image; in accordance with the determined at least one of the digital images being associated with the event, suggesting an identification of the unidentified person as the at least one identified person.

[0051] In accordance with an aspect of the present invention, there is provided a method of suggesting an identification of an unidentified person in a received digital image, the method performed by at least one computer comprising or interfacing with a database of portraits and associated digital images, each portrait associated with an identified person shown in the respective portrait, the method comprising: determining that a respective portrait of at least one identified person shown in at least one of the digital images satisfies a comparison threshold with a portrait of the unidentified person determined from the received digital image; extracting non-portrait visual information from the determined at least one of the digital images; in accordance with a determination of the extracted non-portrait visual information satisfying a comparison threshold with non-portrait visual information from the received digital image, suggesting an identification of the unidentified person as the at least one identified person.

[0052] In this respect, before explaining at least one embodiment of the invention in detail, it is to be understood that the invention is not limited in its application to the details of construction and to the arrangements of the components set forth in the following description or illustrated in the drawings. The invention is capable of other embodiments and of being practiced and carried out in various ways. Also, it is to be understood that the phraseology and terminology employed herein are for the purpose of description and should not be regarded as limiting.

BRIEF DESCRIPTION OF THE DRAWINGS

[0053] Embodiments will now be described, by way of example only, with reference to the attached figures, wherein:

[0054] FIG. 1 illustrates a particular embodiment of the system of the present invention incorporating a social network service to perform targeted distribution of photos.

[0055] FIG. 2 further illustrates the system illustrated in FIG. 1, wherein users add new digital images from various devices over time.

[0056] FIG. 3 illustrates the face recognition method of the present invention, in one aspect thereof, for generating face "signatures" that are compared with signatures of known persons.

[0057] FIG. 4 illustrates linking the results of a face detection, eye detection and face recognition technique in a face database on the storage device of the local computer system.

[0058] FIG. 5 illustrates how peer groups can grow and evolve over time as the list of known persons grows.

[0059] FIG. 6 illustrates potential methods of correcting errors that may result from the automatic face detection, eye detection, and face recognition steps.

[0060] FIG. 7 illustrates a system and method for providing the automatic selective dissemination of photos between users of the invention in the same peer group.

[0061] FIG. 8 illustrates an example embodiment of the graphical user interface that may enable browsing of photos and the face database managed by the computer program.

[0062] FIG. 9 shows face images for known persons plus Boolean operators to narrow the field of photos.

[0063] FIG. 10 illustrates an optional advertising display capability provided by the GUI.

[0064] FIG. 11 illustrates the texture-based face detection method of the present invention, in one aspect thereof.

[0065] FIG. 12 illustrates a method for eye detection, in one aspect of the present invention.

[0066] FIG. 13 illustrates the face recognition method, in one aspect of the present invention.

[0067] FIG. 13a illustrates the face recognition method, in one aspect of the present invention.

[0068] FIGS. 14A, 14B, and 14C illustrate a method of isolating eyes in a photo.

[0069] FIG. 15 illustrates an example configuration of the system of the present invention.

[0070] FIG. 16 illustrates an interface for enabling a user to confirm the identity of a face appearing in an image.

[0071] FIG. 17 illustrates a means by which a user may delete false positive face detections in an image.

[0072] FIG. 18 illustrates a means by which a user may reposition detected eye coordinates corresponding to a face in an image for the purpose of increasing accuracy of the detection algorithm.

[0073] FIG. 19 illustrates the process of manually tagging a face in an image.

[0074] FIG. 20 illustrates a video scanning method whereby frames of video are extracted and face detection is performed on these frames.

[0075] FIG. 21 illustrates one aspect of the present invention wherein a remote web browser or mobile device is enabled to access a proxy server, providing a connection to the functions of the present invention.

[0076] FIG. 22 illustrates deletion of a false positive face detection error.

[0077] FIG. 23 illustrates one aspect of the present invention wherein faces are located in an image which captures the xy coordinates of the location of the faces providing a method to capture a face and adjust the image of the face both in terms of size and rotation to create a portrait – either full size or thumbnail.

[0078] FIG. 24 illustrates copying the image of the face from a photo adjusted in terms of size and rotation and embedding the same in to an advertising message or in to a photo of a product.

[0079] FIG. 25 illustrates using an image to overlay on a photo over the face of a subject to hide negative memories.

[0080] FIG. 26 illustrates the display of faces captured from photos in historical order.

[0081] FIG. 27 illustrates the display of faces/portraits captured from photos and embedding the same in to games and exercises.

[0082] FIG. 28 illustrates the creation and use of a family tree to be an index for photos.

[0083] FIG. 29 illustrates the use of group photos to be an index for photos.

[0084] FIG. 30 illustrates the displays the delivery of face signatures of missing children and wanted criminals.

[0085] FIG. 31 illustrates the matching of face signatures to find people who look alike.

[0086] FIG. 32 illustrates the workflow to create a customized advertisement.

[0087] FIG. 33 illustrates the workflow to create a customized product.

[0088] FIG. 34 illustrates the workflow to hide a negative memory.

[0089] FIG. 35 illustrates the workflow to create customized games and exercises.

[0090] FIG. 36 illustrates the workflow to create a family tree.

[0091] FIG. 37 illustrates the workflow to use a photo as an index.

[0092] FIG. 38 illustrates the workflow to find a missing person.

[0093] FIG. 39 illustrates the workflow to find a look alike.

[0094] FIGS. 40-45 illustrate workflows in accordance with aspects of the invention to use metadata to enhance face recognition results.

[0095] FIG. 46 illustrates a relationship diagram showing frequency of identified persons appearance together, in accordance with an aspect of the present invention.

[0096] FIG. 47 illustrates displaying photos in a tiered list format in accordance with an aspect of the present invention.

[0097] FIG. 48 illustrates a collage of photos representing the tiers shown in FIG. 48.

[0098] FIG. 49 illustrates displaying a timeline of face portraits for an identified person, in accordance with an aspect of the present invention.

[0099] FIG. 50 illustrates identifying a face in a photo by using clustering in accordance with an aspect of the present invention.

[00100] FIGS. 51-53 illustrate face grouping and clustering in accordance with an aspect of the present invention.

[00101] In the drawings, embodiments of the invention are illustrated by way of example. It is to be expressly understood that the description and drawings are only for the purpose of illustration and as an aid to understanding, and are not intended as a definition of the limits of the invention.

DETAILED DESCRIPTION

Overview

[00102] The present invention, in one aspect thereof, provides a networked computer architecture enabling the automatic distribution of images relating to a plurality of individuals operating computer systems on the network.

[00103] The present invention, in another aspect thereof, provides a computer program operable to enable each of the individuals to interface with the networked computer architecture herein provided for sharing information including images. The computer program enables the individuals to upload images including images having depictions of the faces of one or more persons. The computer program may perform a face detection technique to detect the one or more faces in the image, which may result in the generation of one or more face signatures, each face signature corresponding to one of the faces. The computer program may then access a database, wherein the database links face signatures with a list of known persons, each known person being associated with one or more face signatures. Each detected face signature may be provided to the individual as associated to the corresponding known person, or where the face signature is not associated with any known person, that information can be provided by the individual. The individual may be provided a means to confirm the association between a face signature and a known person.

[00104] The present invention, in yet another aspect thereof, provides a novel method for generating face signatures based on faces depicted in images. Further provided is a means for reducing error rates in associating recognized face signatures with one or more face signatures linked to a database.

[00105] The present invention, in a further aspect thereof, enables the automatic selective distribution of images depicting faces. If the faces detected in the images are associated with a person that interfaces with the networked computer architecture herein provided, the computer program herein provided may automatically transmit the image to the person's computer for presentation to the person. It should be noted that the terms "photo" and "image" are used interchangeably herein.

[00106] The present invention, in a further still aspect thereof, provides a novel advertising method that is operable with the networked computer architecture herein provided.

Networked Computer Architecture

[00107] The present invention, in one aspect thereof, provides a networked computer architecture enabling the automatic distribution of images relating to a plurality of individuals operating computer systems on the network. FIG. 1 illustrates an example implementation of the networked computer architecture of the present invention. A plurality of individuals may each connect to the Internet (11) through computer terminals operable to access the Internet (11). The Internet (11) connection enables the transmission and reception of digital data from Internet connected devices, each of which may be operable as provided below.

[00108] The present invention, in another aspect thereof, provides a computer program operable to enable each of the individuals to interface with the networked computer architecture herein provided. FIG. 15 illustrates an example configuration of the system of the present invention. The user (13) of the invention may register, download, and install the computer program to its computer system (15).

[00109] The computer program may, in one aspect thereof, allow the user (13) to invite and establish relationships with other users of the invention. The computer program may, in another aspect thereof, request ads from a set of advertising web servers (23) that deliver ads to the computer program for display to the user (13) on various portions of a graphical user interface ("GUI"). The computer program may, in yet another aspect thereof, transmit photos and metadata related to those photos to other users or to third-party websites the meta data can be stored in the EXIF or similar file header or be embedded inside the jpg or similar image file format in a manner similar to stenographic techniques (25) such as FLICKR™ and FACEBOOK™. These third-party websites (25) may encourage the use of their websites by publishing application programming interfaces (API's) to enable connection from client software or other web-based applications to their service.

[00110] The components of the computer program enabling implementation of the present invention may include:

[00111] A processing engine that may run as a background process on the operating system. It may scan for new digital photos that the user has uploaded or copied to the specified folders on the local and/or a remote or cloud computer that are being monitored for photos, or it may automatically detect new photos when removable media, such as a memory card, is inserted into the computer. When a new photo is detected the face detection, eye detection and face recognition steps may be performed, as described more fully below. The results may be stored in a database such as the database described more fully below. It should be noted that the processing engine

could be executed on a remote computer or cloud service computer, such as where the computer program of the present invention is provided as a service, which may use the software-as-a-service model.

[00112] A GUI that may provide a user with the ability to navigate photos, train the application by identifying known persons, edit and correct the automatic results of the engine, create and modify albums based on search criteria, add peer group members, and send albums to third party websites, each such action described more fully below.

[00113] A database (such as a SQL database, for example) that may be located on a user's computer or on a remote computer or cloud computer, and may contain the results of the face detection, eye detection and face recognition steps described below. The database may also contain metadata for photos and people as well as relationships between known persons and the associated face images.

[00114] The GUI, the processing engine, and the database may be provided on one or more devices. FIG. 21 illustrates one aspect of the present invention wherein a remote web browser or mobile device (83) is enabled to access a proxy server (81), providing a connection to the functions of the present invention. The GUI may be provided on a mobile device (83) such as a PDA or cell phone and perform the face detection and recognition and and indexing and transmit information back and forth to a remote engine running on a website, server, or a user's desktop or laptop computer. In such an implementation, the PDA or cell phone may be provided with a facility for performing face recognition, browsing of images and a facility for uploading images that are captured using a camera incorporated on the device. Uploading may be performed in accordance with the general uploading processes described more fully below.

[00115] The steps performed by the user using the computer program may include:

[00116] Specifying the folder(s) to monitor for new digital photos.

[00117] Training the application by identifying the names and metadata associated with faces found in the digital photos.

[00118] Correcting the errors made by the application; both false positives and false negatives.

[00119] Creating albums (collections of photos) by specifying search criteria including date ranges, Boolean combinations of known persons (via face selection),

EXIF tags, and general tags. Optionally, the user may drag and drop individual photos or groups of photos to the album.

[00120] Once an album is created the user may then specify various output options including:

[00121] Third party websites such as Flickr™ and Facebook™.

[00122] Slideshow formats such as Microsoft™ Powerpoint™ files.

[00123] Document formats such as Adobe™ PDF™ files.

[00124] Inviting other application users to join in a peer group, specifying the options related to those relationships in the peer group, and accepting invitations to join a peer group for another user.

[00125] The networked computer architecture may also include one or more servers to enable techniques described herein. For example, the face detection and recognition method provided herein may be enabled by the servers. The servers, which may be provided on one or more server systems, may include server programs that enable the functions of the servers, including one or more of the following:

[00126] A registration server having a database enabling association of a list of email addresses, associated dates, and other administrative data. The registration server may present an interface such as a webpage to the user for collecting the registration data and then writing this data to the database. The user may then be given a means for installing the computer program described above, such as by being provided with an URL for downloading the client software.

[00127] An ad matching server may accept encrypted requests containing the demographic information for the user. This server may also accept ads in a plurality of formats (such as .JPG, .GIF, .SWF, etc.) from advertisers. For each ad submitted to the application the target demographic for the ad may also be recorded. The ad requests may be matched with the inventory of ads based on the target demographic data. Pointers (unique ID #'s) may be returned for matching ads to the requesting client software.

[00128] An ad delivery server may accept encrypted requests containing pointers to ads. The application may find the ad referenced by the pointer and return that ad to the requesting client software.

Peer Groups

[00129] Referring again to FIG. 1, a first user (13) of the invention may download the computer program from a website or be provided with any other installation means for the installing the computer program. The first user (13) may install the computer program, which may enable the system of the present invention on their laptop or desktop computer system (15) running an operating system (such as the MICROSOFT™ WINDOWS™, APPLE™, or LINUX™ operating system) or the program may be run within a browser such as Microsoft™ Internet Explorer™, Mozilla™ Firefox™, Google™ Chrome™, Apple™ Safari™ or mobile browsers and as a result the program is executed within the browser and on the back-end webservers.

[00130] The first user (13) may define friends (17) in a peer group by specifying their email address to the invention. The computer program may subsequently send an email invitation requesting that a friend (17) also download or otherwise enable the installation of the computer program. After installation, a corresponding computer program for the friend (17) may present to the friend (17) a pending request to join the peer group started by the first user (13). The friend (17), who may now be a second user (17), may be required to approve the connection to the peer group. Once approved, the computer program run by the first user (13) and the second user (17) can now exchange photos as well as metadata about those photos and about known persons, in accordance with the image sharing methods herein described.

[00131] The peer group may be expanded by the first user (13) or the second user (17) by inviting more people (19, 21) to join the peer group. The second user (17) may also create a new peer group that the first user (13) is not part of, and expand that peer group separately. There may be a "many to many" relationship between people and peer groups. Thus the first user (13) can be a member of multiple peer groups and the second user (17) can be a member of multiple peer groups. This enables the easy sharing of photos with other users based on peer group membership.

[00132] As described more fully below, the present invention, in one aspect thereof, enables a known person list. Known persons may optionally be added to one or more peer groups, as described above.

[00133] Peer groups may enable sharing of photos, metadata about photos, and known persons. The GUI may enable creation, modification and deletion of peer groups by a user. The GUI may also enable association of a face image or thumbnail of a known person into an existing peer group, for example by enabling a user to drag the face image or thumbnail over an

area of the interface, such as a field or icon, representing the peer group. A user could assign a representative face image that is associated with their name and that face image is shared and distributed to show up in all peer group contact lists.

[00134] The computer program may generate an invitation each time a friend is added to a peer group. Alternatively, the user may manually add an invitee's metadata to the peer group if the invitee is not part of the known person list. The invitation to an individual may be sent to the invitee via email. For individuals that have installed the computer program of the present invention on their computer system, the email, once received, may prompt the invitee to accept the invitation. Optionally, the individual will be required to enter a code in the computer program to accept the invitation.

[00135] If the friend has not yet installed the computer program or is not registered in the cloud service implementation of the present invention on their computer system, the email, once received, may include a link register or to download or otherwise enable installation and activation of the service and may provide directions for installing the computer program on a computer system. Following successful installation of the computer program the new user may be presented with the invitation, and may accept the invitation to join the peer group in accordance with the steps described above.

[00136] Once the invitation is accepted by the invitee, the invitee may be added to the peer group. The update may be disseminated over the networked computer architecture to enable the corresponding peer group information to be updated in the computer program of each person associated with the peer group.

[00137] In accordance with the face detection technique described below, the peer group may enable automatic selective dissemination of information across the networked computer architecture. The dissemination technique is also more fully described below.

Face Detection

[00138] The present invention, in one aspect thereof, provides a novel method for generating face signatures based on faces depicted in images. FIG. 3 illustrates a face recognition method in accordance with the present invention, in one aspect thereof. A user (13) may provide images to a computer system (15) operable to enable the execution of a computer program. The computer program may monitor file folders associated with the computer system (15) via operating system notifications that may be generated when new files are added or existing files are modified. When new images are found (28) they may be queued (29) for processing.

[00139] Faces in the photos may be located (31) by using any one of multiple techniques that may include: generating face coordinates, which may define a bounding box around the face; determining eye coordinates based on the face coordinates; and creating face signatures (33) for the face based on the face and eye coordinates and by using a face signature technique. The face signature technique may be Principal Component Analysis (PCA), which is known to those skilled in the art. The face signatures may be compares to known face signatures (34) and the photos may be automatically and selectively disseminated to other users (36). Further details of these aspects of the invention are provided below.

[00140] FIG. 4 illustrates linking the results of a face detection, eye detection and face recognition technique in a face database on the storage device of the local computer system or alternatively can be in a face database on the storage device of the cloud computer system . The results may be the coordinates of the associated object. In the case of face detection, the coordinates may define the outline of the face (37) with top left, top right, bottom left and bottom right pixel locations on the original photo which is referred to as a bounding box. In the case of eye detection, the coordinates may represent the pupil location (35) of the left and right eyes. In the case of face recognition, the result may be a face signature (42).

[00141] The graphical user interface (GUI) for the invention may display the face (37) and eye (39) locations on each image (35). As described more fully below, the present invention, in one aspect thereof, provides a list of known persons. If the face signature (42) corresponding to a detected face is associated with a person listed in the known persons list, the GUI may indicate such an association to the user using a graphic notation on or around the image. Otherwise, the GUI may indicate that there is no such association to the user using another graphical notation on or around the image. In the example depicted by FIG. 4, the known faces may be identified with check marks (41) and the unknown faces with the symbol "X" (43).

[00142] Initially all faces may be unknown to the system until the user "trains" the invention to recognize faces. The training method may involve the user. The user, via the GUI of the invention, may use the mouse or other input device to identify the face as belonging to a specific person, by clicking anywhere on the visual bounding box surrounding the face and dragging the face over top of the person's name (or an icon representing the person). Alternatively, the user may drag the icon representing that person over top of the target face. In yet another alternative, the user may click anywhere on the visual bounding box and select a function for identifying a previously unknown face, which may enable the user to enter data related to that person such as name, email address and other details, which may collectively be referred to as

metadata corresponding to the person. This training step may be performed once for each known person. The signature that was created for the face may then enable comparison of all of the unknown face signatures in the face database with the person identified. Both the method for comparison and the method of face detection, eye detection, and face recognition are described more fully below.

[00143] The present invention, in a further aspect thereof, facilitates an optimal training stage by ordering the unknown faces such that the user can identify groups of detected faces that are most likely associated with a single individual. For example, an algorithm could be used to cluster similar faces together based on face signatures. The similarity may be based on certain aspects of their face signatures even when the faces are not already associated with an individual in the face database. Thus a user can identify a cluster of faces as belonging to a particular known person and thereby optimally carry out the training method described above.

[00144] The present invention, in a further aspect thereof, facilitates an optimal training by more than one face signature associated with a person thus improves accuracy by supporting multiple poses of a person and addresses changes to the persons face due to aging, glasses or changes to the face such as caused by a beard or mustache.

Association of Faces with Known Persons

[00145] FIG. 16 illustrates an interface for enabling a user to confirm the identity of a face appearing in an image. A face signature in an image may be within a similarity threshold to a face signature associated with a known person. In this case, an association may be made between the detected face and the known person. One method of comparing face signatures is described more fully below.

[00146] If there is an association between the face and a known person, a further association may be created in the database between the face signature and the known person. Every previously identified face for every known person may be compared with each new face processed by the system. When viewing the faces related to a specific known person, any suspected matches generated by the invention may be displayed and the user may be asked to confirm that the matches are correct.

[00147] Over time, as the number of identified faces increases, the overall accuracy of matching new faces with the correct person may increase since there will typically be many different views of a person with each new face. In accordance with the method of comparing

face signatures provided herein, the number of false positives therefore typically decreases over time.

[00148] FIG. 5 illustrates how peer groups can grow and evolve over time as the list of known persons grows. The list of known persons (101) grows as the user works with the invention, because the user may continue to associate unknown faces with known persons.

Dissemination

[00149] The present invention, in another aspect thereof, provides a computer program operable to enable each of the individuals to interface with the networked computer architecture herein provided for sharing images. FIG. 2 further illustrates the system of the present invention. A user (13) may capture digital images and periodically copy them from one or more image device storage systems (27) to a computer system (15). The user (13) may configure the computer program to monitor specific file folders on the computer system (15) for new images, by inputting the names of the file folders to the computer program using a GUI as described above.

[00150] In accordance with the novel method for face recognition provided by the present invention, the present invention, in one aspect thereof, enables the automatic selective dissemination among a peer group to users whose faces are depicted in images. This is more fully described below.

Detection Optimizations

[00151] The present invention, in one aspect thereof, provides a novel technique for optimizing face detections in accordance with other aspects of the present invention. FIG. 6 illustrates potential methods of correcting errors that may result from the automatic face detection, eye detection, and face recognition steps. The invention uses a novel way of involving the user through the GUI to correct these inevitable errors.

[00152] FIG. 17 illustrates a means by which a user may delete false positive face detections in an image. During the face detection and eye detection phases, there may be false positive errors. These may occur when the face detection technique determines that a face exists even though there is actually no face on the original photo image. To correct these errors the GUI may enable the user to delete false positive errors by moving the face (103) (with the face being identified by a bounding box on the image) over a deletion area (which may be represented by a wastebasket or other representative icon) using a mouse or other input device, by pressing a

keyboard's delete key while the face is highlighted, or by selecting a menu option (105) corresponding to deletion of the face.

[00153] FIG. 18 illustrates a means by which a user may reposition detected eye coordinates corresponding to a face in an image for the purpose of increasing accuracy of the detection algorithm. During the face detection and eye detection phases, there may be errors in eye location coordinates (107). The method of the present invention may determine the eye pupil location and display the eye coordinates (107) visually on the image, but the generated coordinates may not be perfect because they may be an approximation in some cases (for example, a face with sunglasses). The GUI may allow the user to manually reposition the eye coordinates (107), for example by moving the icons (109) representing the eye location with a mouse or other input device. In this way, the accuracy and performance of the invention can be increased as the eye coordinates (107) are typically used to generate a face signature for the face. A change in the eye coordinates (107) may therefore generate a change in the face signature that may significantly affect associating signatures with other with known faces. In addition to the use of eye coordinate the method of the present invention may employ an edge detection technique to align face templates with the detected faces in an image. The alignment method provides another method to confirm the face to reduce false positives. This technique could be performed by aligning the top/bottom and left/right sides of the face with the alignment template and generating a numeric measure of confidence.

[00154] FIG. 22 illustrates deletion of a false positive face detection error. During the face recognition phase, there may be false positive errors related to incorrect association of a face with a known person. A false positive error may result if the invention matches a face signature to a known person and it is not a correct relationship. The GUI may allow the user to drag the face image (111) (thumbnail) over the face image (thumbnail) of the correct known person (113). The invention may then modify the link in the database to show the new relationship between the face and the known person. The old relationship may also be deleted.

[00155] Another category of errors is false negatives. There may be two situations categorized as false negative errors, which are illustrated in Fig. 6:

[00156] 1) Where the system does not detect a face in an image when there actually is a face (47), the GUI may allow the user to draw a bounding box around the face using a mouse, or other input means, and then place both eye locations by using icons representing the eye location. The system may then use the manually entered information to generate a face signature and perform the face recognition method

provided herein. Alternatively, the system may enable the user to manually associate a tag with the face without involving the face detection or recognition process. This manual tagging method may also be used to tag other objects and animals in the images - such as pets - where the human face detection method employed does not result in automatic detection of said object or animal.

[00157] 2) There may also be a false negative error where the system detects a face but the face signature is not matched with any known face signatures even though it is a face of a known person. This may occur if the difference between the signature for the face and any other face signatures for that particular person are too dissimilar. In this case, the system may not automatically detect the relationship and the face may remain unknown. In this circumstance, the GUI may allow the user to drag (49) the face image over the face image of the known person. By doing this the system may link the face image to the known person in the database. With this assistance from the user, the system now has another face signature that will be used for future comparisons with new and unknown face signatures. This may improve the accuracy of the present invention. FIG. 19 further illustrates the process of manually tagging a face in an image.

Automatic Selective Dissemination of Images

[00158] FIG. 7 illustrates a system and method for providing the automatic selective dissemination of photos between users of the invention. When the face of a known person that is a member of a peer group is recognized within a photo (53), the photo (53) may be queued to be transmitted across the Internet (11) in a secure fashion to the peer group member. For example, a first user (13) may upload to their computer system (15) a photo containing the face of a known person that is a second user (17), who is also a peer group member. In this case, when the system determines a face match, the photo (53) may be queued for transmission. Prior to transmission the photo (53) may be reduced to a smaller version and metadata may be included in the digital photo file. The corresponding reduction in size may optimize the use of bandwidth. In a cloud implementation the photo may be physically transferred or the file ownership may be expanded to include the peer group member. The file may or may not be transferred or duplicated.

[00159] The next time the second user (17) accesses the computer program on their computer system (51) it may receive a confirmation request showing a reduced image of the original photo and the associated metadata orthe notification could go to the second user via email also with thumbnails included in the body of the email or as attachments to deliver the

confirmation request. The second user (17) may be prompted whether they would like a copy of the photo (55) on its computer system (51). If the second user (17) responds affirmatively then the system may copy the full image across the Internet from the first user's computer system (15) to the second user's computer system (55) along with the metadata for the photo (55) and the known faces and signatures from the photo.

[00160] Another novel aspect of the present invention uses existing social network service and web-based photo storage sites to share photos with peer group members. The invention may transmit a single photo or group of photos to a target web or cloudbased service. The transmitted photos may already contain metadata from the invention about the people that are in the photos. For example, the social networking site FACEBOOKTM offers the facility to upload photos, share photos, and to manually tag photos to denote which friends are in the photos. The tagging process is manual and time consuming. The present invention may automate such an upload process and eliminate the need to manually tag the photos thereby offering a significant benefit to the social networking user. The present invention may be equally adaptable to other social network service and web-based photo storage sites. As described above, a user may also upload photos directly from a mobile device that incorporates a camera across the Internet.

[00161] Yet another novel aspect of the present invention is that the initial list of known persons can be loaded from the user's social networking account to save further time in configuring the system provided by the present invention.

[00162] FIG. 8 illustrates an example embodiment of the GUI that may enable browsing of photos and the face database managed by the computer program. In this example a user interface is shown with optional banner advertising (57) that could be sold to advertisers. A user may select a photo (123) from an album (125), and the GUI may display thumbnails (121) corresponding to known persons (117) found in the photo (123). Checkboxes (119) may also be used to indicate the presence of the known persons (117) in the photo (123).

[00163] The example depicted in FIG. 9 shows face images for known persons plus the checkboxes for applying Boolean searching such as AND, OR, and NOT selections associated with names of known persons or metadata related to images. A novel feature of the invention is the ability to select photos in a visual manner by allowing the user to click on a thumbnail view of the faces of known persons (59), and applying Boolean operations (61) for each face enabled by checkboxes. This aspect of the GUI enables the creation of an album by combining various search criteria and filters that are applied against the total photo and face database. In a further

embodiment of this invention, the user could assign an image (real, hand-generated or computer generated) to a specific person and that replacement image is overlaid over the portion of every image where that specific person is found.

[00164] Search criteria provided by the computer program may include:

[00165] Folder selection (65), indicating the folder location or file name of photo images on the computer storage device;

[00166] Known persons (67), providing the selection of Boolean operations (AND, OR, or NOT) associated with the faces of the known persons;

[00167] Date range (69), providing the selection of a range of dates corresponding to the photo images to be included in the specific album;

[00168] EXIF data, providing a selection means based on standard photo related information usually appended to the photo by the camera during the photo taking process.

[00169] An alternative method of selecting photos for an album may provide the user the ability to drag and drop individual photos or groups of photos over top of the name of the album (63), or to otherwise associate the photos with the album (63), using the GUI.

[00170] An album (63) may be a group of photos that are saved as a logical entity under the name of the album. The user may specify via the GUI that it wants to send the album to various target file types or locations (71), including a slide show, MICROSOFT™ POWERPOINT™ or other presentation computer programs, ADOBE™ PDF™ or other document file, a web-based sharing site such as FLICKR™ or FACEBOOK™, or a third party printing service.

Advertising Method

[00171] The present invention, in an optional, non-limiting aspect thereof, provides a novel advertising method that is operable with the networked computer architecture herein provided.

[00172] FIG. 10 illustrates an optional advertising display capability provided by the GUI. This is a novel feature of the present invention providing a secure method for simultaneously targeting advertising based on user demographics and maintaining user privacy. The GUI may prompt new users (13) for demographic information that may at a minimum include gender, age and location data. This information may be stored locally on the computer system (15) running the computer program. A request may periodically be sent to a web-based server (73) to return a list of ad pointers. The request may contain an encrypted transmission of the demographic

data for the user. The request may also be signed using a certificate issued by a registration server (77). This latter step may verify the authenticity of the request. The web-based server (73) may conduct a process of matching ads, which are associated with target demographic information, to the requesting user (13) based on their specific demographic information. A list of pointers (i.e. references to ads that exist on different ad servers) may be returned to the requesting user's computer system (15) and passed to the computer program. The computer program may then issue another request to a different web-based server (75) to download the ads referenced by the pointers. The web-based server (73) may then discard the demographic data to protect the privacy of the individual user.

[00173] By separating the web-based servers (73, 77) that perform the ad matching process from the servers (75) that actually deliver the ads, and by not storing the personal demographic data of the user on either of the web-based servers (73, 77), the personal information about the user is significantly more secure than it otherwise would be. The ad delivery servers (75) may store information about ads served for billing purposes but there may be no personal information included in that data. This is a novel implementation for serving ads to any web browser or software program in a secure fashion using demographic data.

Further Implementations

[00174] In another exemplary non-limiting optional aspect of the present invention, another capability of the present invention may enable a computer program to receive digital face images or signatures from the central registration server. For example, an organization seeking to find an individual (such as a missing child or a wanted criminal) may post the individual's face data. Those users that have opted to share their face database may download the data enabling an automatic comparison of the face data with their face database. The organization may be alerted if a match is found between the target individual and a known person for a specific user. This could enable the organization to determine a recent or current location of the individual. It could also enable the organization to determine the name of an individual, since the individual's name may be listed in one or more of the user's known persons list.

[00175] Yet a further embodiment provided by the present invention may enable an individual to find other persons with similar facial features as themselves. Such an application may be useful for a person to find their twin, for example. In this embodiment, a user may submit a photo including an image of their face, from which the present invention may generate a face signature. The face signature may then be compared to other individuals' face signatures that have been previously uploaded. Based on a predetermined similarity threshold, one or more

similar faces may be reported to one or all of the individuals whose faces match. A system in accordance with this embodiment may provide a means for a user to approve contact with others. Matched individuals could choose to send a message to one another if they have specified their approval for such contact. A similar embodiment could be deployed as part of a dating service to match people based on looks.

Face Detection, Eye Detection and Face Recognition

[00176] The present invention, in yet another aspect thereof, provides a novel method for generating face signatures based on faces depicted in images. The face signatures may be generated by using a technique that includes the steps of face detection, eye detection, and face recognition.

Face Detection

[00177] The present invention, in one aspect thereof, provides a method for utilizing a texture-based face detection algorithm as a base method for face detection. One example of a texture-based face detection algorithm is the open source library of routines known as OPENCV™.

[00178] The texture-based face detection algorithm may have a low true-positive rate for specific facial poses, for example rolled frontal faces. This may be due to the texture pattern being trained on frontal face images which differ from the varied facial poses found in normal digital photos. In reality, having a mismatch between the texture pattern used to train the face detection algorithm and the type of poses in the target photos on which the algorithm is applied would result in a higher percentage of errors. Two well-known challenges presently faced in face detection include decreasing false-negative errors in the case of rolled frontal faces and reducing false-positive errors while not increasing false negative errors.

[00179] The present invention enhances the texture-based face detection by applying novel techniques involving three steps to improve the accuracy of the face detection process. In the first step a novel application of the known skin color ratio test on a texture-based face detector is provided to improve the accuracy of the detector. In the second step, a novel method for reducing false-positive face objects is provided by reducing the size of detected face object regions to a predefined size. In the third step, a novel face orientation compensation method is provided.

[00180] FIG. 11 illustrates the texture-based face detection method of the present invention, in one aspect thereof.

[00181] In one particular implementation of the texture-based face detection method, in the first step, the texture-based face detector (131) may initially be set for a high target true positive rate which has a corresponding high false positive rate. The texture-based face detector may be run with the entire photo image as input. The results from this run may give a list of potential face objects in the photo. Any candidate face regions detected may be recorded in a database. For a color photo, a skin color detection test (133) may be performed on the potential face objects to reduce the false positive rate. This skin color test may compare the ratio of the face object area containing skin color to the total area of the object. If the ratio does not exceed a pre-determined threshold then the potential face object may be skipped (135).

[00182] In the second step, detected face object regions that result from the first step may be reduced to a predefined size (such as 44 by 44 pixels). On these reduced regions, the texture-based face detector may be run again (137). The goal of this step is to reduce false-positive face objects. By running on a small size (such as 44 by 44 pixels) input region, false positive errors from incorrect texture patterns from non-faces may be reduced while true positive texture patterns may be preserved. This may result in a reduction in the false positive rate of face detection while preserving the true-positive rate. Face objects that are deemed to be faces in the second step may be accepted (143) as true faces. Those that do not pass this second step may be passed to a third step.

[00183] In the third step, a face orientation compensation method is provided. In the second step described above, in which face detection is performed on smaller regions of the image, the true positive rate may be reduced in the case of rolled faces. The texture pattern in rolled faces may be deemed to be a non-face by the face detector due to the size reduction applied in the second step. To preserve the true positive rate in rolled face cases, face orientation compensation (139) may be performed together with face detection. In this method, the local image region is rotated with an incremental angle and each angle instance may be run through the face detector. One example implementation would rotate the image 2 degrees starting at -20 degrees from the vertical axis and repeating the rotation through +20 degrees from the vertical axis. If rotated face regions are recognized and exist in instances with consecutive incremental angles then the local image region may be determined (141) to be a true face.

[00184] These modifications to a texture-based face detection algorithm may significantly reduce the false positive error rate.

Eye Detection

[00185] FIG. 12 illustrates a method for eye detection, in one aspect of the present invention. The eye detection method applies novel techniques to improve the accuracy for detecting the pupil locations in detected face regions. The first step may be to reduce the overall face region to a smaller region (an "eyemap") (145) that would likely contain the actual pupil/eye locations. A formula may be used to crop the eyemap region from the face region. For example, the formula used to crop the eyemap region may be to remove .23w on the left, .23w on the right, .55h on the bottom and .30h on the top; where w is the width of the face region and h is the height of the face region. FIG. 14A illustrates a particular embodiment of the method of cropping the eyemap region from the face region.

[00186] Furthermore, if the face was detected in the third step of the face detection method on a specific angle instance, then the angle of rotation may be applied (147) to the eyemap region to enable a more accurate selection of the eye locations.

[00187] FIG. 14B illustrates that the formula used to crop the eyemap region may be altered to ensure that the eyemap region is large enough to ensure satisfactory pupil detection results.

[00188] Once the eyemap region has been cropped, the eyemap region may then be re-sized to a fixed size (such as 80x80 pixels) (149) so that a fixed template color variation method may be applied to determine the candidate eye locations. This method may be based on the darker intensity of the pupil relative to the surrounding area of the eyemap region.

[00189] The middle of the color intensity image may be set to zero/black (151) in the intensity map to remove potential pupil candidates that typically result from light reflecting off lenses and the frames of glasses. FIG. 14C illustrates this process.

[00190] The color variation image may be obtained from the color intensity image and may then be passed through a threshold filter so that only a small percentage of the eye region is white (for example, a 2% threshold may be applied) (153). Next, a "best fit" method may be applied to choose the eye locations with the highest intensity of color variation (left and right side). The best candidate pupil location coordinates may be passed along (155) to the face recognition method of the present invention.

Face Recognition

[00191] FIG. 13 illustrates the face recognition method, in accordance with aspects of the present invention. Face recognition may generally be performed through pre-processing (157), projection (159), distance calculation (163) and aggregation (167). Principal Component Analysis (PCA) may be employed by the face recognition method. PCA is a known method,

used abundantly in all forms of analysis because it is a simple, non-parametric method of extracting relevant information from confusing data sets.

[00192] The present invention may employ PCA in a novel way that overcomes its traditional issues with respect to high sensitivity to subject lighting and pose, given that personal photos may have little variation in pose since most subjects may tend to look directly at a camera. The present invention may take advantage of the fact that sets of photos depicting particular persons may be taken over a variety of pose and lighting conditions. The present invention provides a method of aggregating the comparison between the target unknown face and this plurality of faces associated with each known person.

[00193] Pre-processing (157) may first be applied to the image. The face region and eye coordinates provided as input to the face recognition phase may be used to normalize the face region. The normalization process may include translating, rotating and scaling the face region to a predetermined template size. The normalization process may use the eye coordinates as reference points such that the face region image is adjusted to place the eye coordinates on specific image pixels. A standard fixed masking process, potentially limiting the face region to the area inside an ellipse, may then be applied to the image to filter out non-face portions. A flattening process, involving running a two dimensional linear regression on the intensity of the pixels in the face region, may be used to ensure pixel intensity is spatially uniform across the image. Finally, a histogram image equalization (an image processing method known to those skilled in the art whereby the contrast of an image is adjusted using the image's histogram) may be performed in the greyscale domain.

[00194] Projection (159) may then be applied to the image. The resulting pixels of the normalized face region may be passed through a PCA-based formula to create a PCA vector that is used as the face signature by the invention. The PCA vector may comprise a projection image resulting from principal components extracted from a large set of generic images.

[00195] The face signature created from this method may be an array (from the PCA vector) of real numbers of a given dimensionality. Although the exact dimensionality of the vector space may be determined adaptively with its maximum value set to the value capturing, for example, 95% of the input image energy, the default value used may be a dimensionality in the range of 50 to 100.

[00196] Finally, looping (161) may be applied to match the unknown face with a known person. Each face signature (represented as an array of numbers) may be mathematically

compared to any other face signature using linear or non-linear classification logic to determine a distance value (163). For example, two signatures may be compared by computing a normalized inner product distance.

[00197] To compare a face to all of the faces associated with a known person, all of the individual one-to-one comparisons may be made, and then either all of the results may be used in the next step or a set of best matches as determined by comparison to some threshold (165) may be used. The threshold chosen may be chosen such that on average half of the distances obtained when comparing a face to a non-matching person are kept.

[00198] Some form of aggregation may be used to combine the set of distance values obtained in the previous step to determine the distance between the face and a known person. This aggregation may be the computation of the geometric mean of the distance values (169). The geometric mean may be an averaging technique similar to an arithmetic mean, but it may be computed by multiplying the N numbers to be averaged and then taking the Nth root of the product as the desired average. The closest match between the face and each known person may be found by computing this aggregate distance (167) between the face and each known person in the database and choosing the minimum distance.

[00199] Finally, the closest match distance may be compared (171) against a static or dynamically determined threshold to reduce the rate of false positive matches. If a dynamically chosen threshold is used, this threshold may be determined by first assuming the aggregate distance values obtained when comparing a face to a non-matching person having N associated faces are normally distributed (for each possible value of N), and then using the inverse cumulative normal distribution function to compute a threshold which ensures that, on average, a fixed maximum number of or fixed ratio of the unknown faces are falsely matched to a known person. This threshold may vary from person to person as the number of faces, N, associated with each person changes. The advantage of this dynamic threshold calculation includes that the fixed maximum number (or ratio) may be kept as small as possible to limit false positive matches while maintaining an acceptable level of true positive matches for the user.

[00200] FIG. 13a also illustrates the face recognition method, in accordance with aspects of the present invention. The face recognition method shown may normalize a face based on eye coordinates. Each face may be defined by a bounding box determined by the face recognition method. The pixels based within the bounding box may be extracted to create an image of the face. The face image may be recorded to a database and associated with the respective source image from where the face image was extracted. The a PCA vector for the normalized

face may then be calculated and stored in a database. The PCA vector may be compared against the known faces in the database. If a match is found, a face pointer may be stored in memory, such as temporary memory. If after looping through all of the known faces in the databases a match is not found, then the face recognition method determines whether a face was found in the search. If no face was found, then the face recognition ends. If a face was found, then the face recognition method may determine the best match in memory if more than one face match is found. The face recognition method determines whether the best match exceeds a threshold for closeness, as described above. If the threshold for closeness is exceeded, then the best match is written to the database. If the threshold for closeness is not exceeded, then the face recognition ends.

[00201] The present invention, in a further aspect thereof, facilitates an optimal training by more than one face signature associated with a person thus improves accuracy. The invention may allow the user to select the representative subset of known faces for a given individual and thus over-ride the subset chosen by the invention. That subset would then be used by the recognition engine to determine suggested matches and ignore other known faces for that person. Examples where this would be beneficial would be where there multiple poses of a person. It also addresses changes to the persons face due to aging, glasses or changes to the face such as caused by a beard or mustache. By selecting more recent photos as the representative subset, the probability of successful automatic selection for future photos would increase. As the number of face signatures grows that are linked to known people in the local face database, the accuracy of the invention may increase in detecting known people automatically in future photos that are processed. This is a novel feature of this system.

[00202] The invention may learn a face by determining the closest match for a previously identified face from the group of known persons. An advantage of the present invention is that as the number of face signatures linked to known persons in the local face database grows, the accuracy of the invention may increase in detecting known persons automatically in future photos that are processed.

Video Scanning

[00203] FIG. 20 illustrates a video scanning method whereby frames of video are extracted and face detection is performed on these frames. A number N may be set (where N is adjustable) such that video may be scanned every N frames (181) of the video as individual photo images (183) where the previously mentioned techniques (185) would be applied to

detect and recognize faces and known persons. The video could then be disseminated in accordance with the techniques provided herein.

[00204] An optional, non-limiting embodiment provided by the present invention enables an individual to find other persons with similar facial features as themselves. Such an application may be useful for a person to find their twin, for example. In this embodiment, a user may submit a photo including an image of their face, from which the present invention may generate a face signature. The face signature may then be compared to other individuals' face signatures that have been previously uploaded. Based on a predetermined similarity threshold, one or more similar faces may be reported to one or all of the individuals whose faces match. A system in accordance with this embodiment may provide a means for a user to approve contact with others. Matched individuals could choose to send a message to one another if they have specified their approval for such contact. A similar embodiment could be deployed as part of a dating service to match people based on looks.

Face and Portrait Extraction and Creation

[00205] FIG. 23 illustrates the creation of thumbnails or portraits in one aspect of the present invention. Where faces are located in an image 23a one aspect of the present invention captures the XY coordinates of the location of the faces shown in image 23a providing a method to capture a face and adjust the image of the face both in terms of size and rotation to create a portrait, which may either be full size or a thumbnail. As illustrated in Figure 23 the coordinates may define the outline of the face with top left, top right, bottom left and bottom right pixel locations on the original photo which is referred to as a bounding box. The XY coordinates are recorded in the database as illustrated in Figure 11.

[00206] As illustrated in FIG. 23, the faces are located as shown in image 23a and a corresponding bounding box for each located face determined by the XY coordinates is established and recorded in the database as illustrated in Figure 11. As shown in images 23b and 23c of FIG. 23, the XY coordinates to make the bounding box may be adjustable to make subsequent creation of the bounding box, the area around the face, larger or smaller. Using eye location and identification as depicted in Figure 18 by reference numbers 107 and 109, the face may be rotated to make the face vertical as shown in image 23d of FIG. 23.

[00207] The record of the portrait/thumbnail image 23d may be recorded in the database as illustrated in Figure 13 for future use.

[00208] In accordance with at least one exemplary implementation of the present invention, at least one computer terminal, server, or other computing device may detect at least one face in at least one digital image. The computer may determine and store area co-ordinates of a location of the at least one detected face in the at least one digital image. The computer may apply at least one transformation to the at least one detected face to create at least one portrait of the at least one detected face. The computer may rotate the at least one portrait at least until the at least one portrait is shown in a vertical orientation and a pair of eyes of the at least one face shown in the at least one portrait are positioned on a horizontal plane. The computer may then store the rotated at least one portrait. Each detected face may correspond to a person. A copy may be made of or extracted from the portion of the digital image comprising the detected face prior to the application of the at least one transformation.

[00209] An identification of a person may be associated with each stored face portrait in a database stored at or linked to one or more computers.

[00210] Where a digital image shows more than one person, the one or more computers may associate relationships between identified persons based at least partly on respective identified persons being included in the digital image.

Advertising and Product Personalization

[00211] FIG. 24 illustrates merging portraits or thumbnails adjusted in terms of size and rotation and embedding the same into an advertising message or product, or any other type of marketing material or image. The thumbnail or portrait 24a, also illustrated in Fig 23 as image 23d may be adjusted in size to match the size requirements of an advertisement 24b. For example, the computer may apply at least one additional transformation to the at least one stored portrait for matching a portrait size requirement of the marketing image.

[00212] FIG. 32 illustrates the workflow for the creation of the advertisement. As illustrated in Figure 32 when an advertisement is to be personalized one aspect of the present invention matches an advertisement retrieved from an advertisement server database 32b to a user which is retrieved from the user demographic and portrait database 32a. The portrait retrieved from the user demographic and portrait database 32a may be resized at 32c to match size requirements of the advertisement retrieved from the advertisement server database 32b. The user portrait can be merged with or overlaid on top of the advertisement to display a personalized advertising message. In addition to the portrait, the user's name or other information pertinent to the advertisement message may also be merged with or overlaid on top

of the advertisement to display a personalized advertising message as demonstrated by the advertisement 24b.

[00213] Figure 33 illustrates the workflow for the personalization of a product. As illustrated in Figure 33 when a product is to be personalized one aspect of the present invention matches a product retrieved from product database 33b to a user which is retrieved from the user demographic and portrait database 33a. The portrait retrieved from the user demographic and portrait database 33a is resized at 33c to match the size requirements of the product retrieved from the product server database 33b. The user portrait can be merged with product to display the personalized product 24c shown in FIG. 24. In addition to the portrait, the user's name or other information pertinent to the product may also be merged with the product to display a personalized message as demonstrated by the resulting personalized product 24c.

Face Substitution

[00214] FIG. 25 illustrates using a selected image to overlay on a digital image photo to cover the face of a subject, also known as face substitution. An application may be to hide negative memories.

[00215] Figure 34 illustrates a workflow for face substitution. When a user wants to hide negative memories one aspect of the present invention may matche faces in the face database 34a to be hidden in the photos from the photo database 34d with an image that is selected or provided by a user which is stored in the negative memory image database 34b. The databases 34a, 34b, and 34d may be found on one computer server in a single database, in separate databases on the same computer, or on databases stored on or across multiple computers. The image retrieved from the negative memory image database 34b is resized 34c to match the size requirements of the faces to be hidden in the photos 25a retrieved from the photo database 34d. The image is merged with photo 25a such that when the photo is displayed the image hides the face of the negative memory as demonstrated by the resulting hidden face photo 25b. In a non-limiting aspect of the present invention, one or more computers may receive a selection of at least one face to be suppressed, optionally as any form of user input. The one or more computers may then mask the area co-ordinates corresponding to the location of the at least one face to be suppressed in the at least one digital image.

[00216] Optionally, the masking may comprise overlaying a selected image over the area co-ordinate corresponding to the location of the at least one face to be suppressed. Optionally, the one or more computers may adjust the selected image to correspond to size of the area co-

ordinates to be masked. Optionally, the one or more computers may adjust edges of the overlayed image to blend with image characteristics of the at least one digital image. For example, the edges of the overlayed image may be blurred or the opacity of the edges may be modified. Optionally, the image characteristics to be blended may include one or more of color, intensity, brightness, and texture. Optionally, the selection of the at least one face to be suppressed may include a command to suppress a particular individual from being displayed in any digital image, the method comprising identifying any digital image comprising a face corresponding to the particular individual (identified person) to be suppressed and flagging the identified digital images to mask the area co-ordinates corresponding to the location of the at least one face to be suppressed. This may be accomplished by directly modifying the respective digital image(s) or updating associated metadata or other information or data to cause a display of the respective digital image(s) in a non-destructive manner such that the original source digital image is not permanently modified in the database. Accordingly, as mask may be applied to the digital image permanently, or the masking may involve modifying metadata of the digital image to cause the digital image to be masked when displayed.

[00217] FIG. 26 illustrates the display of faces captured from photos in historical order, by date associated with the respective photos, optionally in metadata stored with the photo or elsewhere. The respective date may be the date the photo was created, copied from a camera, transferred to a computer system of the present invention, or any other date associated with the photo. With such ordering the selected faces can be merged to create a single composite image as illustrated by 26b. Such faces can also be automatically fed into a morphing application such that the aging of a person can be animated.

[00218] Optionally, date data may be associated with the digital image. Stored portraits corresponding to a common person may be displayed in accordance with the respective associated date data. Optionally, an animated representation may be generated of an evolution of the stored portraits corresponding to the common person over time.

[00219] FIG. 27 illustrates the display of faces/portraits captured from photos and embedding the faces or portraits into games, exercises, or other interactive applications.

[00220] FIG. 35 illustrates a workflow for creating customized or personalized games and exercises using user portraits and photos, in accordance with aspects of the present invention. A user may select a game or exercise to be played from the game database 35c. The invention selects portraits from the portrait database 35a or photo database 35b for display. The portraits or photos are resized at 35d to match the size requirements of the game to be played. The

resized portraits or photos are merged with the game's user interface for the user to play. Databases 35a, 35b, and 35c may be found on one computer server in a single database, in separate databases on the same computer, or on databases stored on or across multiple computers.

[00221] Optionally, the one or more computers may populate an interactive computer game with the stored portraits and relationships. The interactive computer game comprises a photo reminiscence therapy game.

Indexing Systems Automated Using Face Recognition

[00222] FIG. 28 illustrates the creation and use of a family tree to index photos and FIG. 36 illustrates a corresponding workflow. Portraits may be displayed from the portrait database of identified people. The user may drag and drop each portrait on to the family tree at 36b using the relationship template 28b as illustrated in FIG. 28. In a non-limiting example, each user of the system of the present invention may have six basic relationships of mother, father, sibling, spouse, daughter and son, as shown in template 28b. As the user drags portraits on to the family tree the family tree grows to show the new nodes. Optionally new blank nodes are added for the common relationships to the selected node. As more persons are added the family tree expands as users are added and relationships are defined. When the user has dragged all portraits the family tree is completed by eliminating extraneous relationship or persons such as friends and colleagues. Users will likely have friend and colleague relationships that are pertinent to their personal social map but are identified in a modified network map using a similar drag and drop method.

[00223] The family tree 28a which is created may be used as an index to the user's photos at 36d. When a user selects or clicks on a photo a database query will be executed at 36e to display the photos in which the selected person appears.

[00224] Instead of a family tree 28a, other types of organizational structures representing relationships between persons may be presented in a chart format for populating by dragging portraits thereto, or otherwise selecting portraits. For example, a corporate organization chart may be created by providing a blank, or incomplete corporate organization chart. The user may then be presented with portraits from the database for placement on the chart.

[00225] In accordance with a non-limiting aspect of the present invention, at least one computer may include or interface with at least one database that stores a plurality of portrait images. Each portrait image may be associated with an identified person shown in the

respective portrait. The identification of the person may be stored in the database, another database, or in metadata associated with the respective portrait image. The at least one computer may display the respective portrait of at least one identified person associated with a user. The at least one computer may display a visual representation of at least one personal relationship to the user. The at least one computer may assign at least one of the displayed portraits to at least one of the displayed personal relationships, in accordance with a received user input. The at least one computer may store the personal relationship assignments in the database. The visual representation may include a representation of a tree organizational structure with a plurality of tree nodes, such as for a family tree, where each tree node corresponds to one of the at least one personal relationships. The at least one computer may spawn a tree node for the visual representation corresponding to at least one additional personal relationship in accordance with a user input adding at least one of the displayed portraits to the visual representation. For example, the family tree structure may grow as additional portraits are added to the tree. The user may then specify a relationship for the newly added portrait, or a default relationship may be assigned, or the at least one computer may attempt to determine an appropriate relationship for the new relationship based at least partly on data found on a social network system to which the user is a member. The database of portraits, or another database accessible to the at least one computer, may include a plurality of digital images, and the at least one computer may index at least a subset of the plurality of digital images in accordance with the visual representation. Accordingly, the family tree structure may be used to link to other digital images featuring members of the family tree. In particular clicking on one member of the family tree may link to one or more digital images showing at least that member of the family tree.

[00226] FIG. 29 illustrates the use of group photos to be an index for photos in the photo database, and FIG. 37 illustrates a corresponding workflow. A user may select a photo or photos from the photo database 37a. The photo selected is recorded as a photo for indexing photos and becomes an index in one aspect of the invention. When a user selects or clicks on a face in the photo the one or more computers may search database 37a or another database for more digital images including the identified person corresponding to the face in the photo the user has selected.

In accordance with a non-limiting aspect of the present invention, at least one computer may include or interface with a database of portraits and digital images, each portrait associated with an identified person shown in the respective portrait. The at least one computer may display at

least one of the digital images and cross-reference the displayed at least one digital image with the database of portraits to create a list of at least one identified person shown in the at least one digital image. The at least one computer may index at least a subset of the digital images in accordance with the list of at least one identified person. In accordance with a user input selecting at least one of the identified persons from the displayed at least one digital image, the at least one computer may display at least one of the respectively indexed digital images. Optionally, the indexing may include displaying visual representations of the indexed digital images organized by identified person.*Solicited and automated search for missing persons*

[00227] In yet another aspect of the present invention, the present invention may enable a computer program to receive digital face images or signatures from a third party server, such as a central person search server. FIG. 30 illustrates displaying the delivery of face signatures of missing children and wanted criminals that a user could elect to use for searching the user's photo database(s) for potential matches. A corresponding workflow is shown in FIG. 38. For example, an organization seeking to find an individual (such as a missing child or a wanted criminal) may post the individual's face data shown in images 30a and 30b. The face data may originate from a person search server 38a. Those users that have opted to share their face database 38b may download the data enabling an automatic comparison of the face data with their face database 38b. The results of the comparison may be displayed to the user at 38c for validation. The user may notify the organization at 38d if a match is found between the target individual and a known person for a specific user. This could enable the organization to determine a recent or current location of the individual. It could also enable the organization to determine the name of an individual, since the individual's name may be listed in one or more of the user's known persons list.

[00228] Yet a further embodiment of the present invention, described in reference to FIG. 31 and corresponding workflow FIG. 39, may enable an individual to find other persons with similar facial features as themselves. Such an application may be useful for a person to find their twin, for example. In this embodiment, a user may elect to submit a photo including an image of their face, from which the present invention may generate a face signature stored in face signature database 39a. The face signature may then be compared to other face signatures that have been previously uploaded to database 39a or to look alike database 39b. Based on a predetermined similarity threshold, one or more similar faces may be reported to one or all of the individuals whose faces match at 39c. A system in accordance with this embodiment may provide a means for a user to approve contact with others at 39d. Matched individuals could

choose to send a message to one another if they have specified their approval for such contact. Another variation on this invention would be to look for people with similar facial features taken separately from the entire face - such as mouth, nose, and eyes.

[00229] In accordance with a non-limiting aspect of the present invention, at least one computer may include or interface with a database of portraits, each portrait associated with an identified person shown in the respective portrait. The at least one computer may receive at least one unidentified portrait and compare a face signature of the at least one unidentified portrait against face signatures of portraits of identified persons known to the user. In accordance with a positive result of the comparing, the at least one computer may prompt the user for confirmation of the positive result. In accordance with the confirmation, the at least one computer may associate the at least one unidentified portrait with the at least one identified person confirmed by the user and store the at least one unidentified portrait in the database.

[00230] Optionally, the unidentified portrait shows a missing person. Optionally, the receiving may include several steps. First, the digital image may be received. The at least one computer may then detect at least one face in the received digital image. The at least one computer may determine and store area co-ordinates of a location of the at least one detected face in the received digital image. The at least one computer may apply at least one transformation to the at least one detected face to create the at least one unidentified portrait of the at least one detected face. The at least one computer may rotate the at least one unidentified portrait at least until the at least one unidentified portrait is shown in a vertical orientation and a pair of eyes of the at least one face shown in the at least one unidentified portrait are positioned on a horizontal plane.

Visualizing Relationships from Photo Metadata

[00231] When a set of digital photos contains name tags that identify the people represented in those photos then there is potential to "mine" that information and generate potentially interesting, entertaining, and useful techniques for displaying relationships between people that have been tagged in those photos. How the name tags are made available to the computer system is not limiting to the concept of using that data to display interesting graphs and charts. One approach to generating the name tags quickly is to use face detection and recognition technology. This technology speeds up the tagging process by automating most of the manual steps. The name tag data could simply exist in the photo metadata, such as in the Adobe XMP format, or it could exist in a SQL or other database.

[00232] FIG. 46 depicts a graph generated in accordance with an aspect of the present invention. The relationships between people appearing in photos are shown by interconnected lines between people. Starting with a central, or selected person (in this example: Ray), the invention shows a node that represents the number of photos in which Ray appears. The node may be sized relatively according to the number of photos. Any nodes attached directly to the central "Ray" node may identify people that appear in photos with Ray. So for example, April appears in 100 photos with Ray, and "Friend A" appears in 135 photos with Ray. Then the next layer of the diagram shows people that don't appear with Ray, but appear with the people connected directly with the Ray node. So, Sandy and Lisa appear together with April in photos. This method is used to graph all relationships moving outward from a central person. Each node may show a frequency of appearance together of the person named at the node and the person named at the immediately preceding node.

[00233] This graph in FIG. 46 could be used as an index to the photos. By clicking on any node in the graph, the corresponding photos represented by that node could be displayed in slideshow or thumbnail list format. The at least one computer could query the one or more photo databases in advance of receiving a click on any of the nodes in order to be prepared to present the corresponding photos, or the at least one computer could perform any such query or queries after having received the click user input.

[00234] In accordance with a non-limiting aspect of the present invention, at least one computer may include or interface with a database of digital images and respective metadata identifying a name of at least one identified person shown in the respective digital image. The at least one computer may select one of the identified persons from the database and determine a count of a total number of digital images where the identified person appears. For each identified person shown in at least one of the digital images with the selected identified person, the at least one computer may determine a count of a total number of digital images where the respective identified person appears with the selected identified person and display a visual representation, such as a graph or chart as shown in FIG. 46. The visual representation could include a first node representing the selected identified person (e.g. "Ray" in FIG. 46) and the respective count of the total number of digital images where the identified person appears. For each identified person shown in at least one of the digital images with the selected identified person, a second node may be presented representing the respective identified person shown in at least one of the digital images with the selected identified person. Each respective node may further include a visual representation of the respective count of the total number of digital

images where the respective identified person appears with the selected identified person. Each second node may be linked to the first node, optionally in the form of a visible line or by other means of displaying a visible link.

[00235] Optionally, for each identified person displayed with a respective second node (a "second person"), for each identified person shown in at least one of the digital images with the respective second person, the at least one computer may determine a count of a total number of digital images where the respective identified person appears with the respective second person. In this case, the visual representation may include, for each identified person shown in at least one of the digital images with the respective second person, a third node representing the respective identified person shown in at least one of the digital images with the respective second person, each respective node further comprising a visual representation of the respective count of the total number of digital images where the respective identified person appears with the respective second person; and a link between the respective second node and each respective third node.

[00236] Another non-limiting exemplary implementation could show the relationships purely in list format based on the tiers away from the central person. FIG. 47 shows how those photos may look arranged by tiers.

[00237] Another non-limiting exemplary implementation for representing the tiers may be to show a collage of photos contained in that tier. FIG. 48 shows a possible display that demonstrates this method.

[00238] Another non-limiting exemplary implementation of the present invention for showing the data available from the name tags in photos is to extract the face of a person from photos and display those faces on a timeline. FIG. 49 provides an example. Starting with a selected person (selected by the at least one computer or in accordance with user input), all faces of that person may be extracted from each photo in which they are tagged and displayed along some form of date or time axis. If more than one photo of the selected person is available, this may show the evolution of a person over time.

[00239] In accordance with a non-limiting aspect of the present invention, at least one computer may include or interface with a database of portraits, each portrait associated with an identified person shown in the respective portrait. The at least one computer may select one of the identified persons from the database, ordering a plurality of the portraits associated with the selected identified person based at least partly on date metadata associated with each

respective portrait, and displaying a visual representation. The visual representation may include a timeline; and an arrangement of the plurality of the portraits along the timeline in accordance with the respective ordering.

[00240] More details regarding use of face detection and recognition for tagging purposes will now be described. Face detection algorithms operate in many different ways, but the net result of scanning a digital image and applying one or more of these algorithms is the presentation of a list of possible face regions. These regions are usually identified by a bounding box defined by four coordinates (e.g. top/left, top/right, bottom/left, bottom/right).

[00241] If a set of new photos is offered to a face detection system of the present invention, then the system may return a list of faces to the user and ask the user to tag the faces – in other words – attach a name to the faces. This name could be input via the keyboard or via drag and drop from an existing contact list or address book. The user may also typically provide input to delete any false positive faces where the system has falsely identified a region of a photo as a face.

[00242] A face recognition system of the present invention may take the face detection results (e.g. a list of bounding box coordinates and a pointer to the original digital image) and generate digital signatures for each face. These signatures are mathematical representations of the pixels that constitute the face as defined by the bounding box or other mask area applied to the bounding box or a subset of the bounding box. For example, it may be possible to use the eye coordinates of the face to center an oval mask over the face region to attempt to eliminate non-specific features like hair, hats, and other non-facial objects. Then only the pixels within this mask area are used to generate the face signature.

[00243] These mathematical signatures could be a sequence of numbers (real or complex) or a single digital string or a multi-dimensional array depending on the algorithm. Other functions performed by a face recognition system of the present invention may be to:

[00244] 1. Compare two face signatures together to determine a "likeness" score. If that score passes a dynamic or pre-defined threshold then it becomes a "suggested" match between the two.

[00245] 2. Combine "like" face signatures together into clusters of faces that are similar. This also uses a dynamic or pre-defined threshold to determine whether face signatures belong together in the same cluster.

[00246] An optional function is to find a representative signature for a single person that has a list of face signatures based on tagging activity by the user. In essence, this person is "known" to the system because faces have been tagged with the same name.

[00247] In accordance with aspects of the present invention, the present invention may enable the visualization of data relationships extracted from photo metadata – specifically name tags and dates that are attached to digital photos. This data could be attached to photos directly via common metadata formats (e.g. EXIF, Adobe XMP, etc.) or could exist separate from the photos in a database that links the photo name to the metadata contained in database tables.

[00248] Based on people identified via the tags (or in the database) and the frequency of appearance and who they appear with in the photos, data relationships are determined that can be graphed in different ways. These graphs provide ways to visualize the relationships.

[00249] The graphs may automatically be created by the invention or the user of the invention may request a graph be created starting with a specific person selected by the user. The specific person would become the center of the graph in a network representation, or left starting point in a "left to right" representation.

[00250] To collect the data required to display a graphic representation like FIG. 46, multiple queries may have to be run against a database containing metadata – specifically the name of people appearing in photos. If the data only existed in the metadata directly attached to the digital photos then this metadata would have to be collected via an image scanning process. The resulting collection could be placed in computer memory (such as an array of text fields) or it could be placed into a permanent or temporary SQL database for subsequent query purposes. For purposes of this part of the description, assume that the data resides in a SQL database.

[00251] The initial query would find a count for all images containing people that appear with the selected "starting" person in one or more photos. We'll call these people "acquaintances". The resulting list could be sorted in descending order based on number of appearances for each acquaintance. The graph would display the starting person as a node in the graph. The size of the node may or may not vary based on the number of photos. The number of photos in this case would be the total number of photos in which the "starting person" appears.

[00252] The next node displayed would be the first or largest acquaintance in the list. The size of the node may or may not vary with the number of times they appear in photos with the "starting person". This node would be attached via a connector to the original starting node.

This process would continue until all the acquaintances are exhausted in the list. One non-limiting implementation would limit the size of the list to a minimum number of appearances together. The graph could represent people that appear in at least 3 photos with the starting person.

[00253] Once the list is exhausted, then for each acquaintance another query would be run to determine all of the people that appear together with that acquaintance but NOT with the starting person. Based on this list then nodes would be added to the graph with connectors back to the acquaintance.

[00254] This process would continue until all acquaintance nodes in the graph are exhausted. In order to limit the size of the graph – especially in the case of a person with tens of thousands of photos - it is possible that the user could specify a limit of X tiers away from the starting person.

[00255] The other types of graphs identified that show this "tier relationship" would be generated in a similar fashion to the above, but the method of display differs. For FIG. 47, the photos may be shown as thumbnails or scrollable images on a "Tier by Tier" basis. This could be a tabbed interface that offered a "tab per tier". For FIG. 48, the photos are shown in a collage format for each tier away from the central starting person. Each collage could be a separate graph or page, or they could be combined into one large graph.

[00256] To generate FIG. 49, the dates for the images may be used to define the ordering of faces along the timeline. The face images themselves may be extracted from the original photos using coordinates for a pre-determined bounding box around the face. The bounding box may be determined based on a face detection method that identifies the coordinates containing a face automatically, or the user may manually define a bounding box by physically drawing a box around the face with the aid of a mouse, touchpad or touch screen user interface.

[00257] In accordance with a non-limiting aspect of the present invention, at least one computer may include or interface with a database of digital images and respective metadata identifying a name of at least one identified person shown in the respective digital image. Each person may have been previously identified using face detection and recognition techniques described herein. The at least one computer may select one of the identified persons from the database, determine at least one first identified person shown in at least one of the digital images together with the selected identified person, and display a visual representation. The visual representation may include, for each first identified person, a first tier node representing

the selected identified person and the respective first identified person being shown in at least one of the digital images together. The visual representation may also include, for each first identified person, a second tier node representing the respective first identified person being shown in at least one of the digital images without the selected identified person.

[00258] Optionally, the visual representation may include, for each first identified person, a second tier node representing the respective first identified person being shown in at least one of the digital images without the selected identified person, but with a second identified person, wherein the second identifier person is determined not to be shown in any of the digital images showing the selected identified person.

[00259] Optionally, the visual representation may include, for each second identified person, a third tier node representing the respective second identified person being shown in at least one of the digital images without the respective first identified person.

[00260] Optionally, each first tier node may include a collage of the digital images that show both the selected identified person and the respective first identified person.

[00261] Optionally, each first tier node may include a collage of digital images that show both the selected identified person and the respective first identified person; each second tier node may include a collage of the digital images that show the respective first identified person without the selected identified person; and each third tier node comprises a collage of the digital images that show the second identified person without the respective first identified person.

Clustering Description

[00262] An optional function of the present invention may be to find a representative signature for a single person that has a list of face signatures based on tagging activity by the user. In essence, this person may be "known" to the system because faces have been tagged with the same name. For purposes of determining a likeness score and suggesting a match between two photos, the representative signature is used to compare with each unidentified face to determine if there is a match. The representative face signature could also be a set of face signatures such that each item in the set may represent a single cluster of face signatures for that specific person.

[00263] Finding a representative face for a group of faces assigned to a person may be useful in order to reduce the time required to compare a large number of known faces (e.g. potentially hundreds of known faces, or more) with each new unidentified face. Furthermore, people age over time and change their appearance for a variety of reasons so using a set of

face signatures representing clusters of similar faces for a particular person can provide better results while at the same time reduce the number of comparisons necessary versus comparing every specific known face.

[00264] A further use of clustering may be to present "like" faces to the user in batches for tagging purposes. This may save time in providing the ability to tag many faces with one name, instead of tagging each individual face.

[00265] One challenge with clustering is that for performance reasons it is not desirable to have to re-cluster the entire set of unidentified faces as new faces are introduced to the set. It may be more efficient to employ various techniques that allow for the creation and management of incremental clusters.

[00266] Details will now be described regarding clustering for the purposes of finding the representative faces for an individual during the recognition step. The plurality of faces associated with a known person may be grouped using a form of hierarchical clustering, where face signatures are compared as described above, to create groups of faces having similar appearance. To compare an unknown face to the known person, all of the individual, one to one, face comparisons may be made, and then the results may be combined by arithmetic mean to form one or more aggregate results, one for each group of similar faces.

[00267] To enable effective comparison of the aggregate results a linear correction which depends on the number of individual results used to compute the aggregate result may be applied. This linear correction may be determined by first comparing a group of known faces having a particular number, "N", with a large number of individual faces known to belong to different people to determine the distribution of results.

[00268] Then the linear correction may be determined to be that which best aligns this distribution to a standard normal distribution. Finally, the correction may be further adjusted so as to give larger groups of faces an advantage in the comparison with unknown faces by either increasing the standard deviation or shifting the mean. This final step ensures that people who appear frequently in a user's collection of photos have an appropriate increase in their likelihood of being suggested as a match for a new unknown face.

[00269] The plurality of corrected aggregate results obtained by comparison of a single unknown face to all of the known persons may be compared against either a fixed threshold or a dynamically chosen threshold. If a dynamically chosen threshold is to be used, it may be selected to be the threshold that yields the maximum number of unknown faces for which only a

single person has results exceeding the threshold. The advantage of such a dynamically chosen threshold is that it maximizes the number of true person suggestions while simultaneously minimizing false positive suggestions.

[00270] In one embodiment of the invention this clustering process could employ a similar method to what is described under the term "hierarchical clustering" in Wikipedia (See: http://en.wikipedia.org/wiki/Hierarchical_clustering). The initial clustering may be "agglomerative" (a bottom up approach where each observation starts with its own cluster, and pairs of clusters are merged as one moves up the hierarchy) while the selection of representative faces may be "divisive" (a top down approach where all observations start in one cluster, and splits are performed recursively as one moves down the hierarchy). Initially every face is considered to be its own separate cluster. Each face is compared to every other face and the score (likeness) values are recorded and sorted. Scores below a certain pre-determined threshold are discarded. Then, starting with the highest score (the two faces that are most alike) and working towards the lowest score, each pair of faces are joined by an edge if they are not already joined via some path of edges. That is, two separate clusters are merged but faces within a cluster are not further joined by additional edges. The result is several distinct dendrograms (trees), each one representing a cluster. Note that within each dendrogram there are no loops and the number of edges is one less than the number of faces. For each cluster where the number of faces is larger than some specific integer threshold (e.g. 20), we select a subset of the faces to represent the cluster.

[00271] Selection of the subset could be implemented as follows. First find the edge with the lowest score and remove it to split the tree into two smaller subtrees. Then decide how many faces will be selected from each subtree so that the counts are in equal proportion to the size of the subtree. For example, if we are looking for 15 faces and subtree A is twice as big as subtree B, then we will want to select 10 faces from subtree A and 5 faces from subtree B. If the number of faces in the subtree is equal to the number we want, then those faces are simply output as the result and processing of that subtree terminates. If the number of faces is greater than the number we want, this process is applied again recursively. That is, within the subtree, the next edge with the lowest score is found and removed to further divide the tree. The result is the reduction of a tree of any size to some fixed size such that the remaining faces are a statistically representative sample of the original set of faces.

[00272] Details will now be described regarding the use of clustering for unidentified faces to improve the time involved for tagging by reducing the number of clicks required by the user. For

practical and performance reasons, in accordance with an aspect of the present invention, a fully incremental constant time clustering algorithm was created. At least one advancement of this clustering algorithm may be the constant time aspect, which does not vary depending on total number of photos in the set. To describe the steps involved in adding a new face to the existing clustering, first assume that each of the existing faces has been assigned some sort of clustering token (e.g. an integer). Two faces are considered to be in the same cluster if they have the same token. Second, assume that each face is associated with some photo and that each photo has a date and time associated with it. This is usually but not always the date and time that the photo was taken. Finally, the photos are kept in a sorted order by this date and time metadata.

[00273] Given a new photo with at least one face in it, first use the date/time of the new photo to find its location within the sorted list of existing photos. Then start performing one-to-one face comparisons between the new face and existing faces by moving outward in both directions from this location. That is, the new face is first compared to existing faces that were photographed at a similar date/time before moving to progressively more distant (past and future) dates.

[00274] If a one-to-one face comparison yields a likeness that exceeds some fixed threshold, then the new face is assigned the same cluster token as the existing face and the clustering of the new face is complete.

[00275] Three rules may be applied to ensure that the time spent adding each new face to the clustering is constant. First, new faces are never compared to other new faces in the same photo. Second, if the new face fails in its comparison to one face of a particular cluster, then the new face is not compared against any other faces from that same cluster. Third, we now have a fixed maximum number of comparisons that will be made. If this number is reached without finding a match, then the new face will be assigned a new cluster token and will, therefore, be the first face in a new cluster.

[00276] Finally, when processing a batch of photos, the photos are processed in a random order to improve "long range" clustering.

[00277] FIG. 50 shows photos and faces with associated dates and times, arranged chronologically. The "New Photo" is being analyzed in accordance with the present invention. The letters on each face represent the cluster id/token for the respective face. The curved lines with arrows shown below the cluster tokens in FIG. 50 represent the face-to-face comparisons

that are to be performed from faces in the New Photo to faces in other photos. The numerical value shown on the curved lines representing the face-to-face comparisons indicates the order in which the respective face-to-face comparisons are performed. For example, photos with the closest date/time to the New Photo may be compared first, and the remaining faces may be compared in chronological order of the associated dates and times of the photos or faces. Assuming no matches were found in earlier face-to-face comparisons, the three existing faces with no curved lines linking the respective faces to the face from the New Photo, indicate that comparisons with those respective faces were skipped, as the respective faces belonged to a cluster already considered.

[00278] In order to show a match, the comparisons cease when a match is found and the new face takes on the same cluster id letter as the matching face (e.g. "E"), shown in FIG. 50.

[00279] In order to show no-match, then the new face may get assigned a new cluster id (e.g. "F"), not shown in FIG. 50.

[00280] In accordance with a non-limiting aspect of the present invention, at least one computer may include or interface with a database of digital images and respective metadata identifying a date of the respective digital image, a plurality of the digital images showing at least one respective unidentified person ("unidentified digital images"). The at least one computer may sort the unidentified digital images by the respective date metadata, and assign a respective clustering token to each of the unidentified digital images. The assigning may include, in accordance with a determination that a subset of the unidentified digital images each show a common unidentified person, assigning a common respective clustering token to each of the unidentified digital images of the subset. The at least one computer may group the unidentified digital images by respective clustering token. At some point, the at least one computer may receive a new digital image from another computer, database, user, or from anywhere else. The new digital image and respective metadata may identify a date of the respective new digital image, and the new digital image may include a new unidentified person. The at least one computer may then attempt to identify the new unidentified person in the received image by using or leveraging any of the clustering techniques described herein. In particular, the at least one computer may perform at least one comparison of the new unidentified person to the at least one respective unidentified person of the plurality of the digital images in an order, wherein for each group of unidentified digital images, the at least one computer may perform only a single comparison of the new unidentified person to the respective common unidentified person. The at least one computer may assign a clustering

token to the new digital image in accordance with the comparison performing resulting in a determination of the new unidentified person common to a respective one of the groups of unidentified digital images. Optionally, the comparison performing order comprises an order by date metadata closest in date to the date metadata of the new digital image. Optionally, wherein upon having performed a predetermined maximum number of comparisons of the new unidentified person to the at least one respective unidentified person of the plurality of the digital images, the at least one computer may halt the comparison performing and assigning a new clustering token to the new digital image.

[00281] FIGS. 51-53 illustrate aspects of the faces clustering of the present invention. FIG. 51 shows faces of a respective known person may be grouped through tagging methods provided by the present invention. In FIG. 51, groups of faces of known persons A, B, and C, are respectively grouped. In FIG. 52, a recognition algorithm in accordance with the present invention may the groups of faces of a known person into one or more clusters of faces of the known person. The splitting into clusters of like faces may be based at least partly on the face signature distance between each face in the group of faces of the known person. In FIG. 53, when an unknown face is submitted to the face recognition method of the present invention, the recognition algorithm of the present invention may compare the unknown face with each cluster for each known person separately.

Using Image Metadata to Improve Face Recognition Results

[00282] A challenge in face recognition may be that due to the unconstrained nature of consumer photos taken with a wide range of camera devices – including smart phones, cell phones, and disposable cameras – the ability to accurately identify people in photos (or video) will likely never reach 100% accuracy. There are just too many variables similar to the challenges associated with accurate weather forecasting.

[00283] It is possible to enhance the accuracy of recognition results beyond the pure mathematics of analyzing and comparing pixels contained in the image. By taking advantage of image related metadata including date taken, camera type, location coordinates, and event information it is possible to reduce false positive data generated from the face recognition algorithms. In a further extension of this concept it is also possible to recognize other objects in the image (non-human) that could relate to a specific place, event or time.

[00284] These concepts also apply to video images in addition to static images. They can be applied in real-time as the user is taking the photo or video; or they can be applied post-image taking.

[00285] A non-limiting implementation of this concept in accordance with an aspect of the present invention in shown in FIG. 40. Face recognition algorithms operate on a list of unidentified faces and compare the digital signatures for those faces against digital signatures for known faces. Any faces from the unidentified set that come within a pre-defined (or algorithmic) threshold with a known face will become "suggested matches" for the person linked to the known face. If a single photo generated five face regions from the face detection scan, then it may be inefficient to have the same person offered as a suggestion for more than one face in the same photo. Note that there could be special circumstances (e.g. photos involving a mirror and photos modified with an editor) where the same person could appear more than once in a single photo, however it is not practical to design a system that satisfies these rare corner cases. Thus, if the face recognition algorithm came up with two (or more) faces from the same image as a suggestion for the unidentified person, then further logic would consider the fact that the two (or more) faces are in the same image and request the "most closest match" to be the suggestion used. Should the most closest match that is suggested to the user be rejected by the user, in order to improve efficiency, it may be desirable to, with respect to any faces not the most closest match from that image, and thus not suggested, discarded those faces from being suggested in any other digital images as well. Any rejected face(s) suggestions may then be compared against the set of known people excluding the unidentified person to find the next best match (if any).

[00286] In accordance with a non-limiting aspect of the present invention, at least one computer may include or interface with a database of portraits and associated digital images, each portrait associated with an identified person shown in the respective portrait. The at least one computer may determine that respective portraits of at least two identified persons shown in one of the digital images satisfy a comparison threshold with a portrait of the unidentified person determined from the received digital image. The at least one computer may then suggest an identification of the unidentified person as the respective one of the at least two identified persons having a respectively associated portrait that is determined to be a closest match to the portrait of the unidentified person from amongst the at least two identified persons. The at least one computer may then exclude a remainder of the at least two identified persons from being

subsequently suggested from any other one of the digital images as an identification of the unidentified person.

[00287] Dates or times may also be considered when suggesting faces, as shown in FIG. 41. It should be assumed that the metadata (e.g. dates, coordinates, camera type, etc.) related to the images being used for the present invention is accurate, otherwise basing face suggestions based on the metadata would not be expected to increase accuracy. Consider a person, referred to as P, tagged in a photo that shares the same date as another photo. In the other photo, assume there exists an unidentified face where two (or more) people meet the recognition threshold for calling that face a suggested match for those people. Then if one of those people that meet the threshold happens to be confirmed by the user to be person P, the present invention may increase the ranking of person P in a list of suggested identifications based on the probability that person P will show up again in photos from the same date after already having been tagged and confirmed to be present on that date in another photo.

[00288] In accordance with a non-limiting aspect of the present invention, at least one computer may include or interface with a database of portraits and associated digital images, each portrait associated with an identified person shown in the respective portrait. The at least one computer may determine that a respective portrait of at least one identified person shown in at least one of the digital images satisfies a comparison threshold with a portrait of the unidentified person determined from the received digital image. In accordance with the determined at least one of the digital images associated with metadata comprising a date corresponding to date metadata associated with the received digital image, the at least one computer may suggest an identification of the unidentified person as the at least one identified person.

[00289] Relationships with people may also be considered, as shown in FIG. 42. Assume a person, referred to as P, is tagged in a photo and other unidentified faces are found in that photo. Further assume that person P also belongs to a group, referred to as C, and this group is known to the system. Then as part of the recognition suggestion algorithm, the fact that the probability of other faces in the photo also being members of group C is higher could be considered in the method by reducing the threshold for each person that is a member of group C, or moving a person from group C higher in the list of potential matches if there is more than one person meeting the suggestion threshold for a given unidentified face.

[00290] In accordance with a non-limiting aspect of the present invention, at least one computer may include or interface with a database of portraits and associated digital images,

each portrait associated with an identified person shown in the respective portrait. The at least one computer may, in accordance with a determination that the received photo comprises at least one identified person associated with a defined group, suggest an identification of the unidentified person based at least partly on a determination that a respective portrait of at least one identified person associated with the defined group satisfies a comparison threshold with a portrait of the unidentified person determined from the received digital image.

[00291] Locations or location coordinates may also be considered, as shown in FIG. 43. Assume a person P is tagged and confirmed to be in a photo in location X on date A, and, per the recognition algorithm, person P would normally be a suggested match for unidentified faces in other photos also taken on date A, but in location Y, where Y is more than N hours away from X. In this case, the suggested match for person P may be discarded on the basis that person P could not have been, or was unlikely to have been, in both locations X and Y within the date timeframe established by the metadata of the respective photos. This may take into account the probability that person P cannot be in two places at the same time.

[00292] In accordance with a non-limiting aspect of the present invention, at least one computer may include or interface with a database of portraits and associated digital images, each portrait associated with an identified person shown in the respective portrait. The at least one computer may determine that a respective portrait of at least one identified person shown in at least one of the digital images satisfies a comparison threshold with a portrait of the unidentified person determined from the received digital image. In accordance with the determined at least one of the digital images associated with metadata comprising both (i) a date corresponding to date metadata associated with the received digital image; and (ii) a location within a predetermined distance threshold of location metadata associated with the received digital image; the at least one computer may suggest an identification of the unidentified person as the at least one identified person.

[00293] Event information, or other information available on a social network, may also be considered, as shown in FIG. 44. Assume the system knows the person P is attending an event X based on social network information captured for that user or other data source, then the probability that person P will appear in photos taken at event X is higher. It is also reasonable to assume that the probability that person P will show up in photos taken at event Y, taking place on the same date, is lower. The recognition method could utilize this further information to assign person P a higher ranking (via one or more specific adjustments) for faces found in photos taken at event X where P would otherwise meet a threshold for being suggested as any

of the unidentified faces. The recognition method could also assign person P a lower ranking (via one or more specific adjustments) for faces found in photos taken at event Y.

[00294] In accordance with a non-limiting aspect of the present invention, at least one computer may include or interface with a database of portraits and associated digital images, each portrait associated with an identified person shown in the respective portrait. The at least one computer may determine that a respective portrait of at least one identified person shown in at least one of the digital images satisfies a comparison threshold with a portrait of the unidentified person determined from the received digital image. The at least one computer may also determine that the received digital image is associated with an event, based at least partly on metadata associated with the received digital image. In accordance with the determined at least one of the digital images being associated with the event, the at least one computer may suggest an identification of the unidentified person as the at least one identified person.

[00295] Non-human object or environmental information may also be considered, as shown in FIG. 45. For example, assume that a person P was confirmed and tagged in a photo, and that photo was deemed to be part of a set X of similar photos based on date, event, or location information. Then if person P was further found in the confirmed photo using an object recognition method to be wearing a green sweater, then that information could be used to apply a higher priority or ranking to person P if a face in another photo from set X was found also to be attached to a green sweater. In addition to clothing, other objects shown in the photo, such as furniture, trees, cars, animals, clouds, vistas, or any other environmental arrangements of photographic details may be analyzed and considered. The color, texture, orientation, or arrangement of any such details may be analyzed and considered. Particularly, if person P tagged in a photo of a set based on date, event, or location, then non-face details of person P may be compared to suggest that person P is an unidentified person in other photos of the set (non-face details may include clothing shape or color, hair color, glasses, skin tone, etc.)

[00296] In accordance with a non-limiting aspect of the present invention, at least one computer may include or interface with a database of portraits and associated digital images, each portrait associated with an identified person shown in the respective portrait. The at least one computer may determine that a respective portrait of at least one identified person shown in at least one of the digital images satisfies a comparison threshold with a portrait of the unidentified person determined from the received digital image. The at least one computer may then extract non-portrait visual information from the determined at least one of the digital images. In accordance with a determination of the extracted non-portrait visual information

satisfying a comparison threshold with non-portrait visual information from the received digital image, the at least one computer may suggest an identification of the unidentified person as the at least one identified person.

Voice-assisted Face Tagging

[00297] Optionally, voice or speech recognition may be used to assist or support face tagging as provided in aspects of the present invention. The at least one computer may prompt the user to tag photos. The user may respond by providing user input using any available means, such as by clicking with a mouse, touchpad, key entry, or by responding with voice input. The user may be interfacing with a local computing device, upon which the face tagging method is operating, or the user may be interfacing with a computer in communication with one or more other computers or computer servers, that alone or together provide for the tagging of photos or faces. In either case, the local computing device with which the user is interfacing, which may be a mobile phone, personal computer, or any other type of computing device, may include or be connected to, either through a wired or wireless connection, a microphone or other audio input peripheral. The local computing device, or one of the other computers in communication therewith, may process the user's audio input to determine one or more voice commands.

[00298] Once the tagging process has begun, and voice recognition is supported and enabled, the user may be presented with one or more photos to tag. Optionally, the user may be asked whether the user recognizes a particular photo. One of the computers may have attempted to determine a date or time of the photo. The user may be prompted to either confirm or modify this date or time. A voice command may be provided from the user in response to be processed by one of the computers. Through the face recognition methods described in accordance with aspects of the present invention, where at least one person is determined to be found in the photo, the user may be prompted to identify the at least one person. A voice command may be provided from the user in response identifying the person by name. Where the voice command does not provide a full name for the person, the face recognition method may suggest a full name to be used to tag the person based on the voice command received. For example, if the user identifies the person as "Bob", the method may suggest at least one full name for "Bob" based on other persons named "Bob" tagged in other photos by the user, or based on other persons named "Bob" who are connected to the user through a social network or contact list. This process may repeat for all of the persons in the photo, and for any other photos not yet tagged by the user. Optionally, existing photos already tagged may also be re-presented to the user for tagging or re-tagging, preferably after all untagged photos have been

processed and tagged in accordance with the method of the present invention. The method may also prompt the user to record a caption for any photos being tagged. Any recorded caption may be played back for the user to confirm prior to applying to the respective photo. The caption may also be processed through voice recognition techniques and saved as a text caption associated with the respective photo. The caption text may also be presented to the user for review or confirmation prior to saving.

General

[00299] It will be appreciated that any module or component exemplified herein that executes instructions may include or otherwise have access to computer readable media such as storage media, computer storage media, or data storage devices (removable and/or non-removable) such as, for example, magnetic disks, optical disks, tape, and other forms of computer readable media. Computer storage media may include volatile and non-volatile, removable and non-removable media implemented in any method or technology for storage of information, such as computer readable instructions, data structures, program modules, or other data. Examples of computer storage media include RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD), blue-ray disks, or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired information and which can be accessed by an application, module, or both. Any such computer storage media may be part of the mobile device, tracking module, object tracking application, etc., or accessible or connectable thereto. Any application or module herein described may be implemented using computer readable/executable instructions that may be stored or otherwise held by such computer readable media.

[00300] Thus, alterations, modifications and variations can be effected to the particular embodiments by those of skill in the art without departing from the scope of this disclosure, which is defined solely by the claims appended hereto.

[00301] In further aspects, the disclosure provides systems, devices, methods, and computer programming products, including non-transitory computer readable memory, or non-transient machine-readable instruction sets, for use in implementing such methods and enabling the functionality described previously.

[00302] Although the disclosure has been described and illustrated in exemplary forms with a certain degree of particularity, it is noted that the description and illustrations have been made

by way of example only. Numerous changes in the details of construction and combination and arrangement of parts and steps may be made. Accordingly, such changes are intended to be included in the invention, the scope of which is defined by the claims.

[00303] Except to the extent explicitly stated or inherent within the processes described, including any optional steps or components thereof, no required order, sequence, or combination is intended or implied. As will be will be understood by those skilled in the relevant arts, with respect to both processes and any systems, devices, etc., described herein, a wide range of variations is possible, and even advantageous, in various circumstances, without departing from the scope of the invention, which is to be limited only by the claims.

CLAIMS

What is claimed is:

Any and all features of novelty disclosed or suggested herein, including without limitation the following:

1. A method performed by at least one computer, the method comprising:

detecting at least one face in at least one digital image;

determining and storing area co-ordinates of a location of the at least one detected face in the at least one digital image;

applying at least one transformation to the at least one detected face to create at least one portrait of the at least one detected face;

rotating the at least one portrait at least until the at least one portrait is shown in a vertical orientation and a pair of eyes of the at least one face shown in the at least one portrait are positioned on a horizontal plane; and

storing the rotated at least one portrait.

2. The method of claim 1 wherein each of the at least one detected face corresponds to a person.

3. The method of claim 1 comprising extracting the at least one detected face from the at least one digital image prior to the applying.

4. The method of claim 1 comprising inserting the at least one stored portrait in a marketing image.

5. The method of claim 4 wherein the marketing image is an advertisement.

6. The method of claim 4 comprising applying at least one additional transformation to the at least one stored portrait for matching a portrait size requirement of the marketing image.

7. The method of claim 1 comprising:

receiving a selection of at least one face to be suppressed;

masking the area co-ordinates corresponding to the location of the at least one face to be suppressed in the at least one digital image.

8. The method of claim 7 wherein the masking comprises overlaying a selected image over the area co-ordinate corresponding to the location of the at least one face to be suppressed.

9. The method of claim 8 comprising adjusting the selected image to correspond to size of the area co-ordinates to be masked.

10. The method of claim 8 comprising adjusting edges of the overlayed image to blend with image characteristics of the at least one digital image.

11. The method of claim 10 wherein the image characteristics may include one or more of color, intensity, brightness, and texture.

12. The method of claim 7 wherein the selection of the at least one face to be suppressed comprises a command to suppress a particular individual from being displayed in any digital image, the method comprising identifying any digital image comprising a face corresponding to the particular individual to be suppressed and flagging the identified digital images to mask the area co-ordinates corresponding to the location of the at least one face to be suppressed.

13. The method of claim 7 wherein the masking comprises applying a permanent mask to the digital image.

14. The method of claim 7 wherein the masking comprises modifying metadata of the digital image to cause the digital image to be masked when displayed.

15. The method of claim 1 comprising associating date data with the digital image; and displaying stored portraits corresponding to a common person in accordance with the respective associated date data.

16. The method of claim 15 comprising generating an animated representation of an evolution of the stored portraits corresponding to the common person over time.

17. The method of claim 1 comprising associating an identification of a person with the at least one stored portrait.

18. The method of claim 17 comprising associating relationships between identified persons based at least partly on respective identified persons being included in the digital image.

19. The method of claim 18 comprising populating an interactive computer game with the stored portraits and relationships.

20. The method of claim 19 wherein the interactive computer game comprises a photo reminiscence therapy game.

21. A system comprising at least one computer comprising at least one processor and a non-transitory computer readable memory comprising processing instructions, that when executed by the at least one processor, cause the computer to:

detect at least one face in at least one digital image;

determine and store area co-ordinates of a location of the at least one detected face in the at least one digital image;

apply at least one transformation to the at least one detected face to create at least one portrait of the at least one detected face;

rotate the at least one portrait at least until the at least one portrait is shown in a vertical orientation and a pair of eyes of the at least one face shown in the at least one portrait are positioned on a horizontal plane; and

store the rotated at least one portrait.

22. The system of claim 1 wherein the processing instructions when executed by the at least one processor cause the computer to extract the at least one detected face from the at least one digital image prior to the applying.

23. The system of claim 1 wherein the processing instructions when executed by the at least one processor cause the computer to insert the at least one stored portrait in a marketing image.

24. The system of claim 1 wherein the processing instructions when executed by the at least one processor cause the computer to:

receive a selection of at least one face to be suppressed;

mask the area co-ordinates corresponding to the location of the at least one face to be suppressed in the at least one digital image.

5

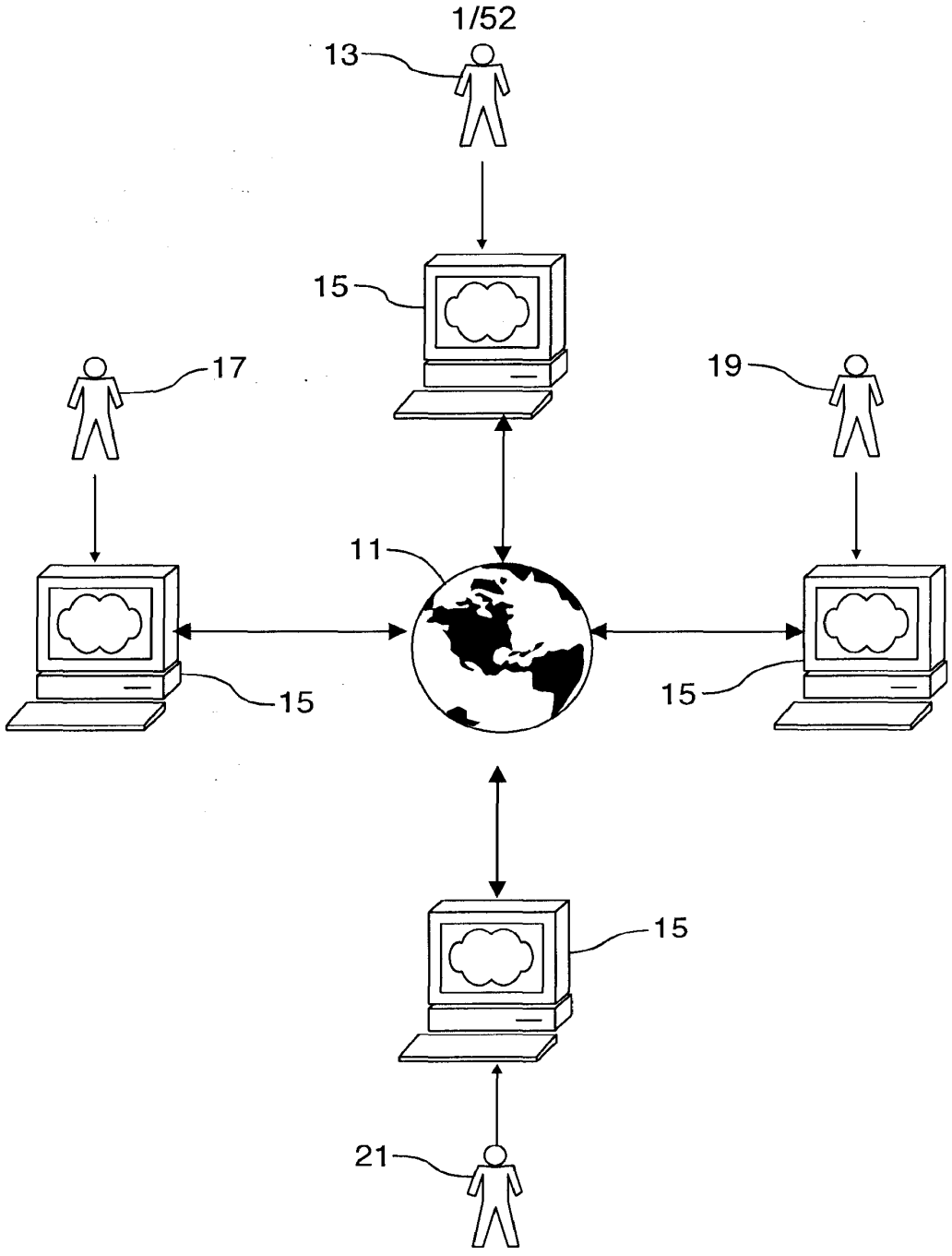


FIG.1

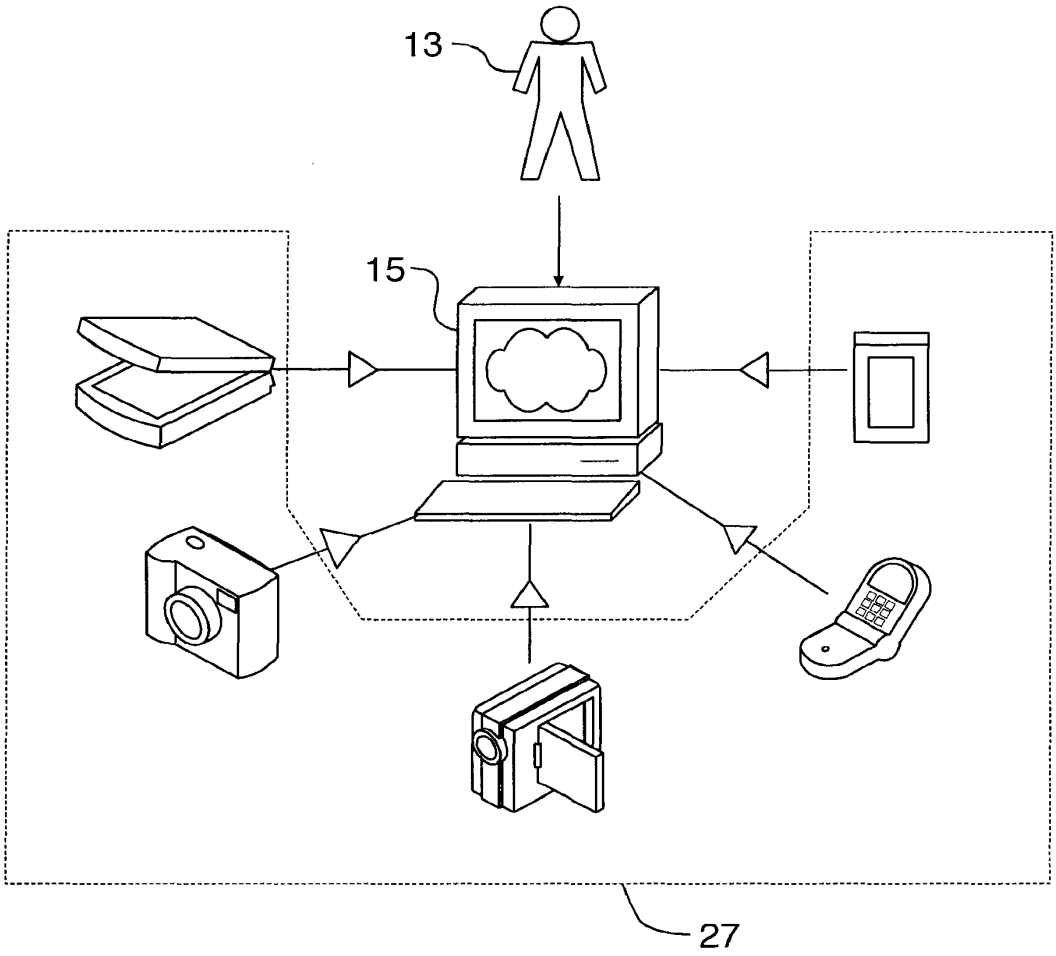


FIG.2

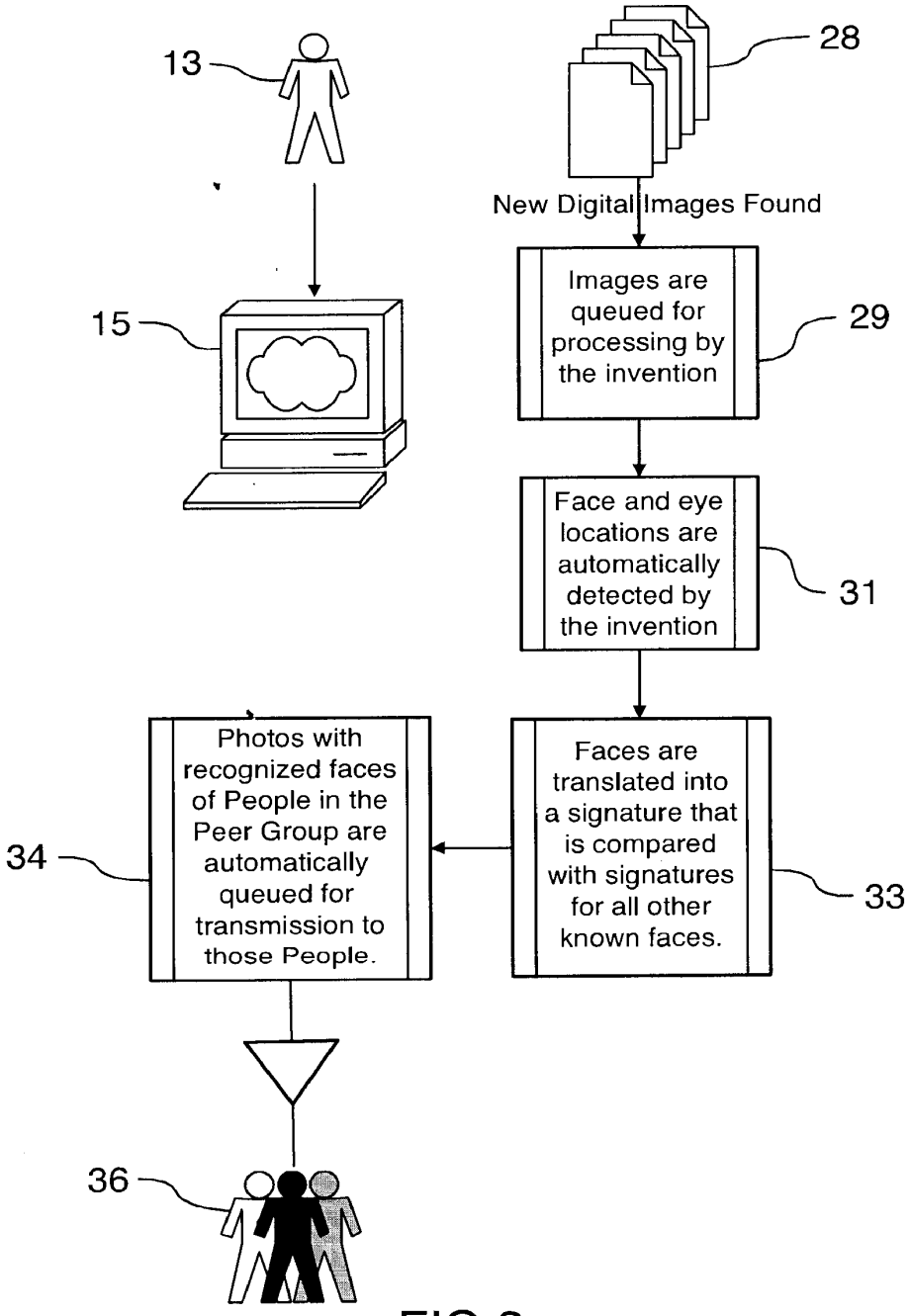

13
28
New Digital Images Found
15
Images are queued for processing by the invention
29
Face and eye locations are automatically detected by the invention
31
Photos with recognized faces of People in the Peer Group are automatically queued for transmission to those People.
34
Faces are translated into a signature that is compared with signatures for all other known faces.
33
36

FIG.3

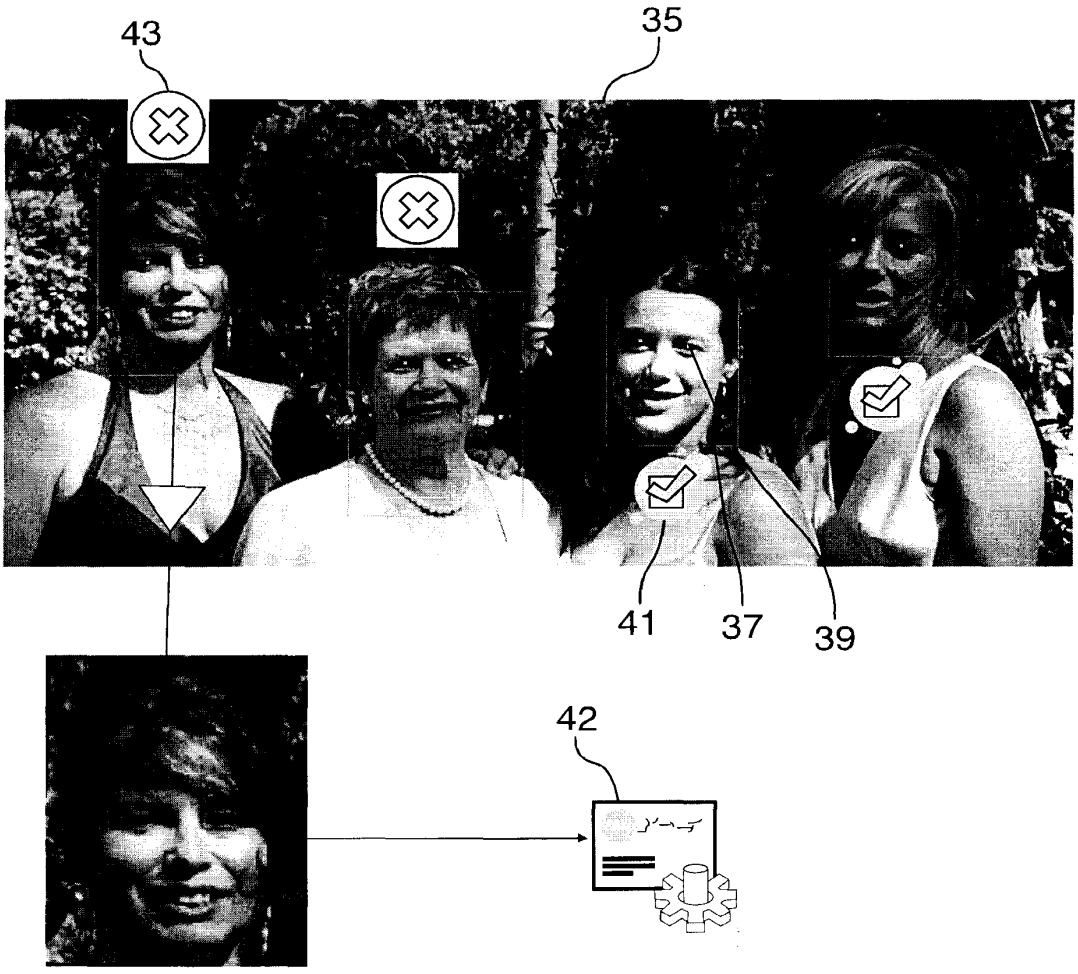


FIG.4

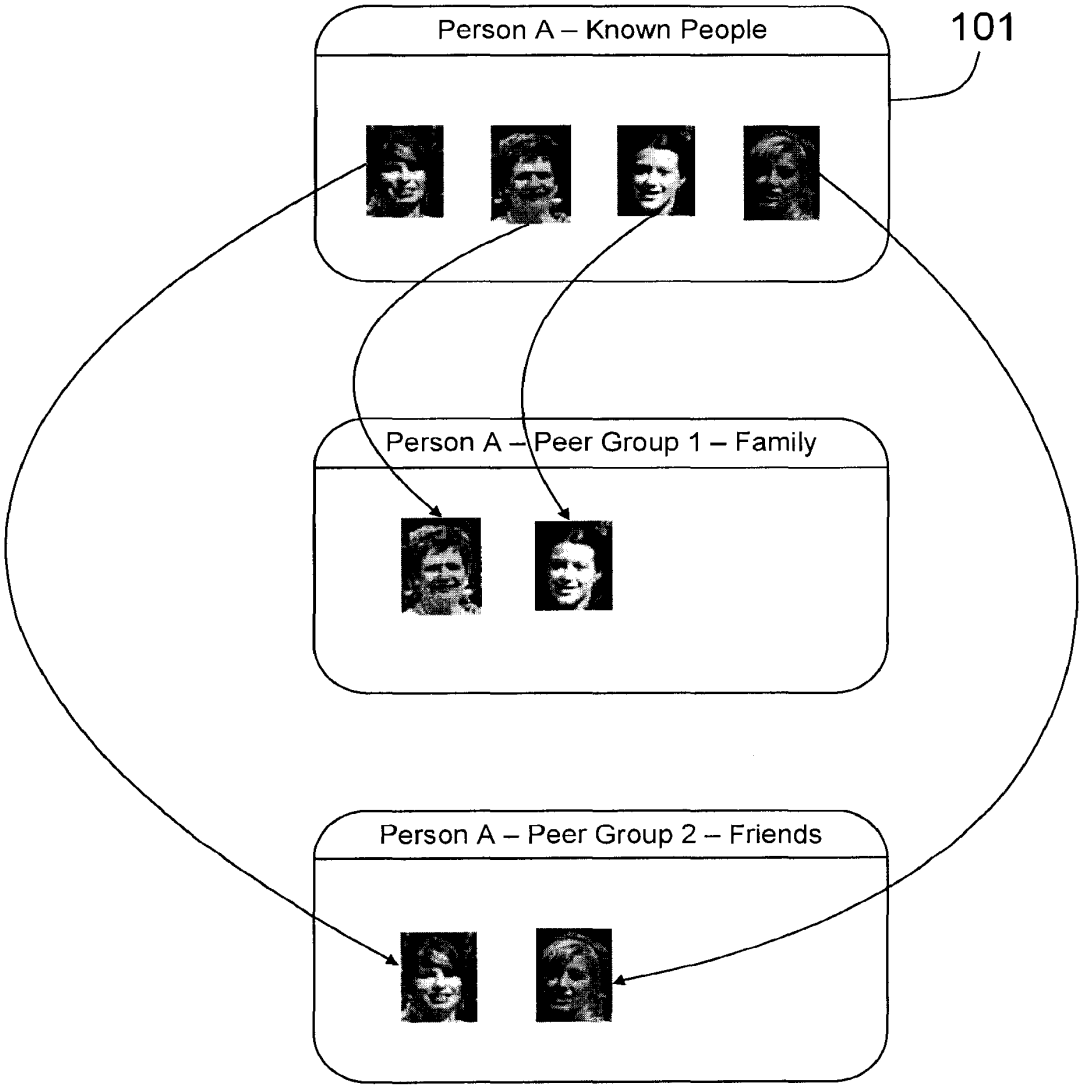

Person A – Known People
101
Person A – Peer Group 1 – Family
Person A – Peer Group 2 – Friends

FIG.5

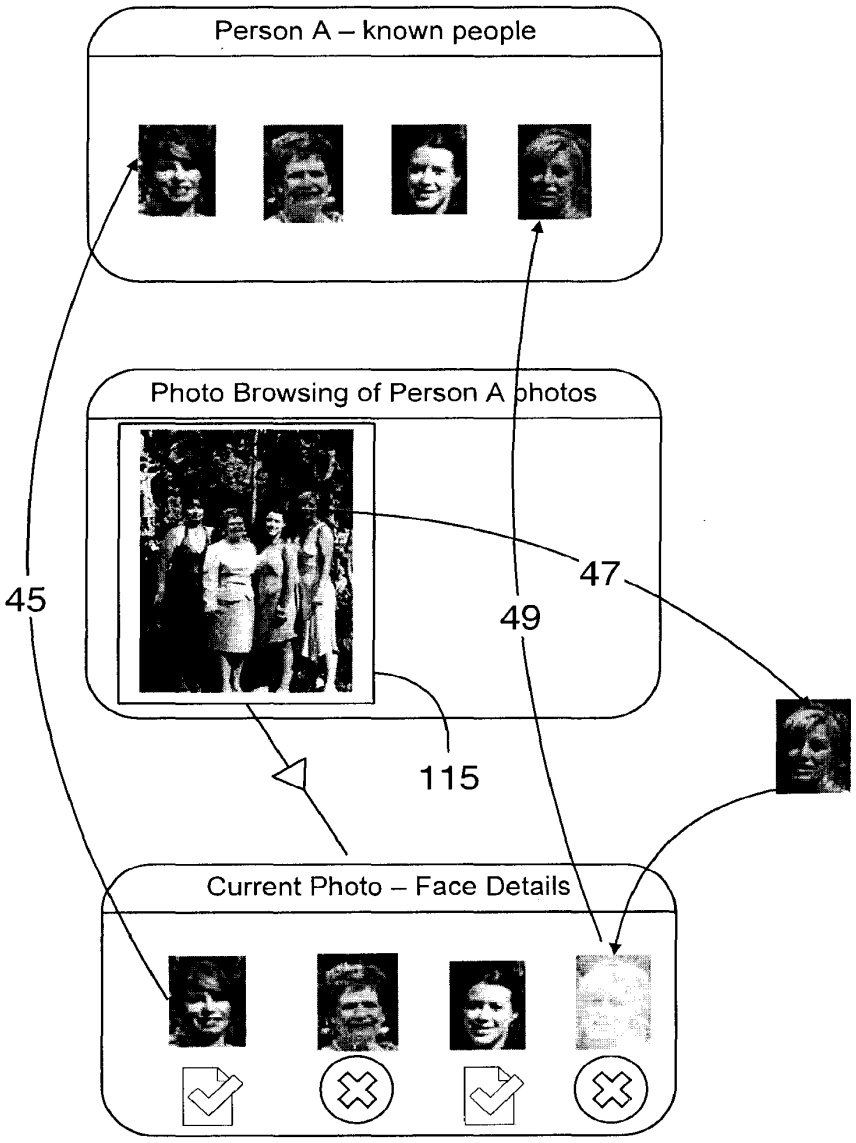

Person A – known people
Photo Browsing of Person A photos
45
47
49
115
Current Photo – Face Details

FIG.6

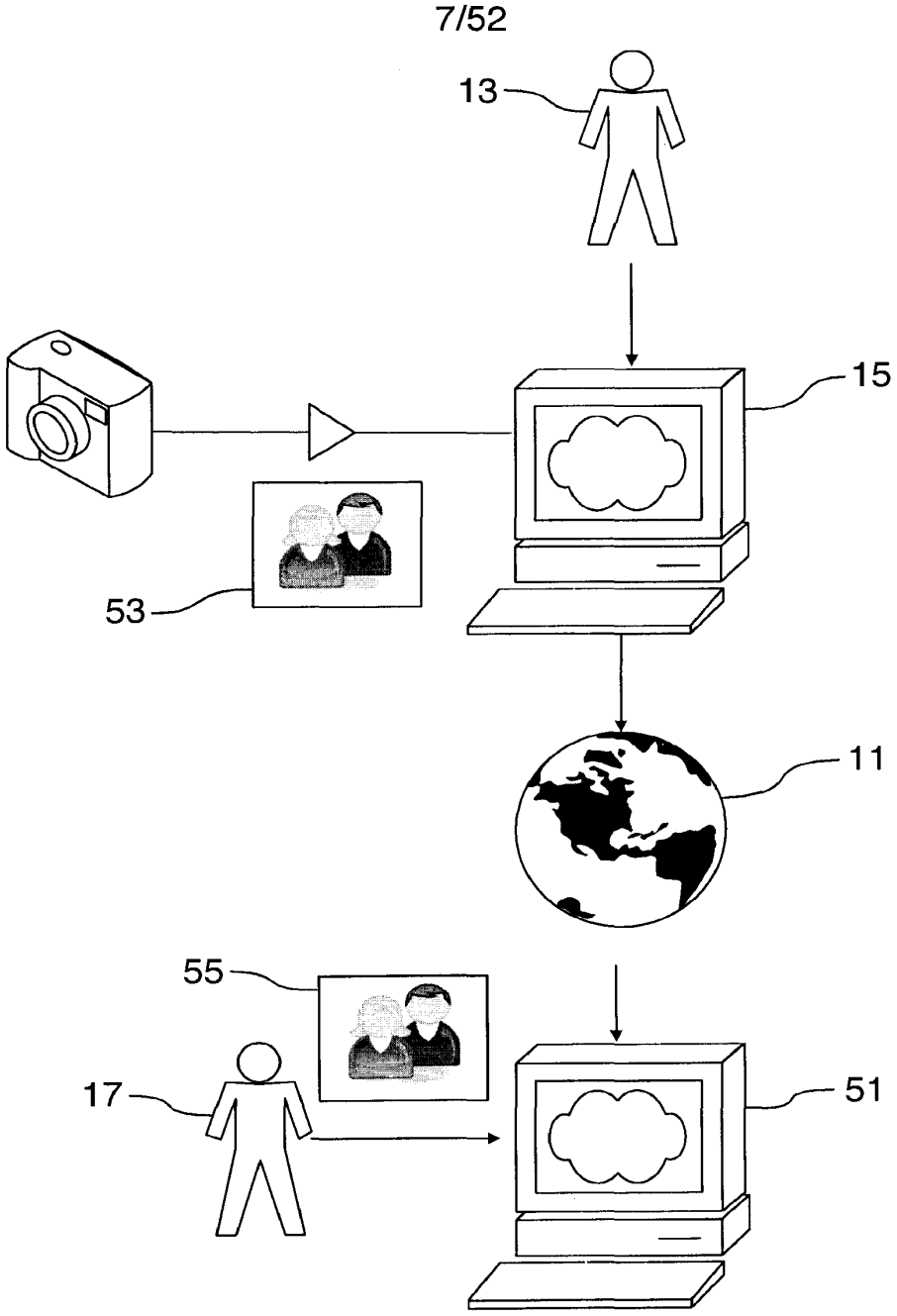


FIG.7

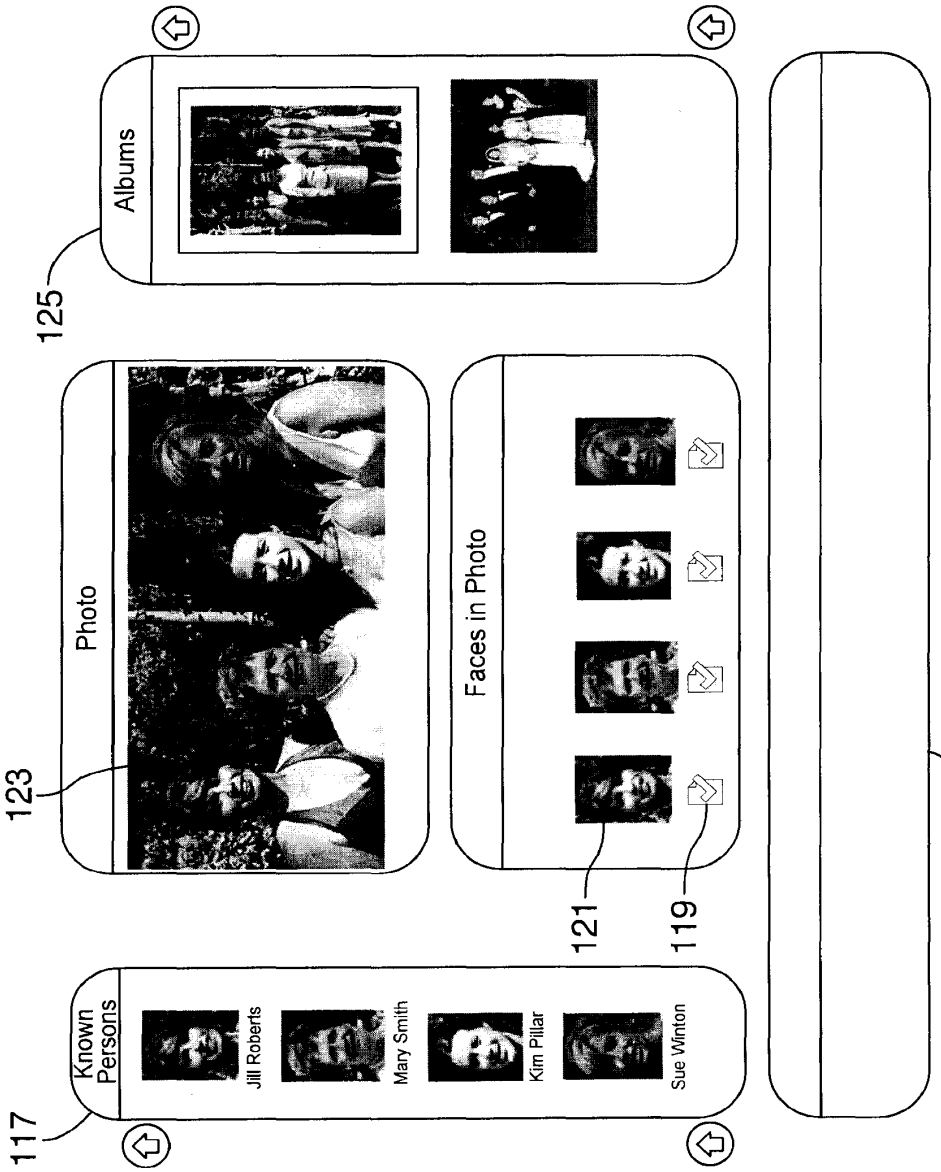

Albums
125
Photo
123
Faces in Photo
121
119
Known Persons
117
Jill Roberts
Mary Smith
Kim Pillar
Sue Winton
57

FIG.8

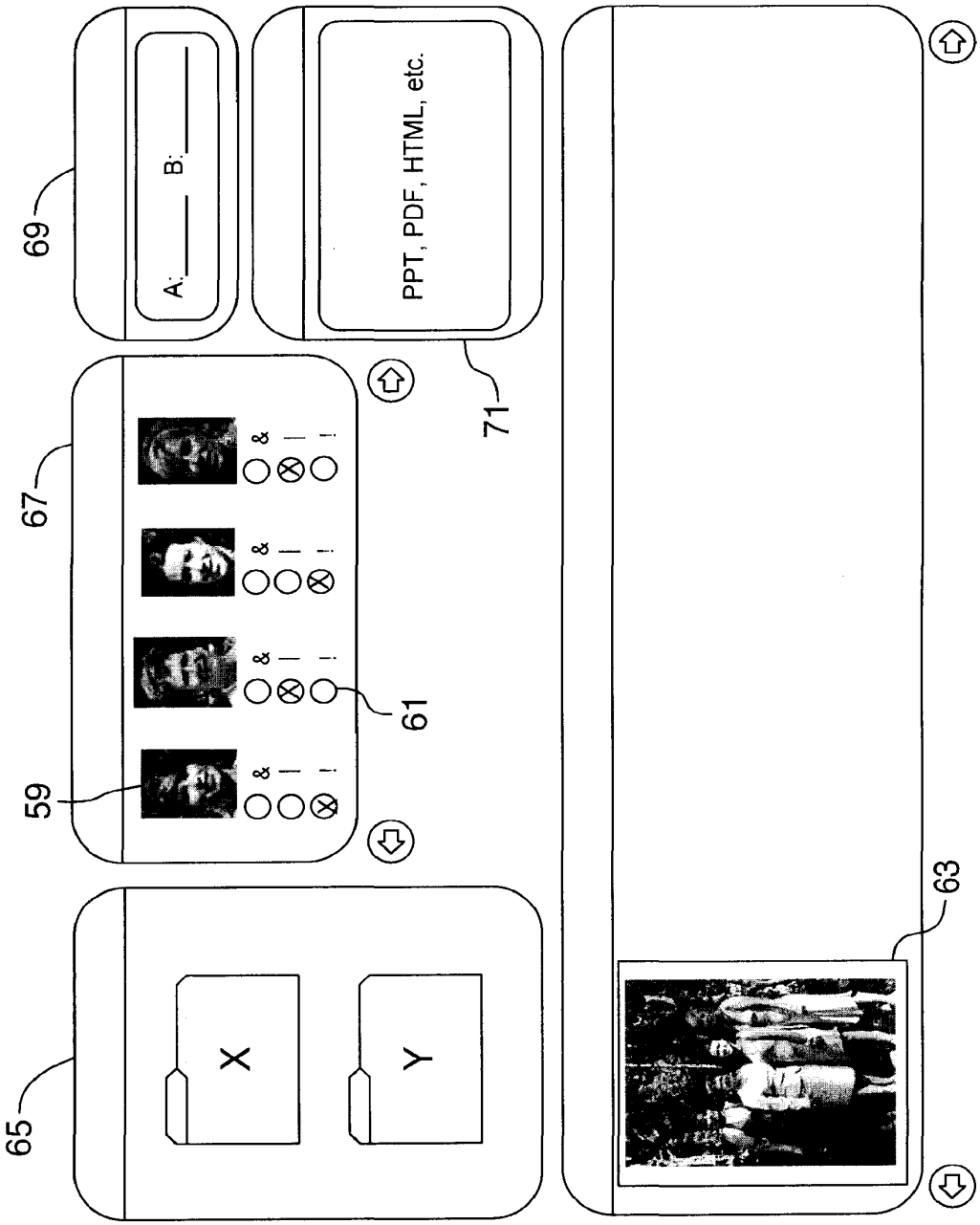


FIG.9

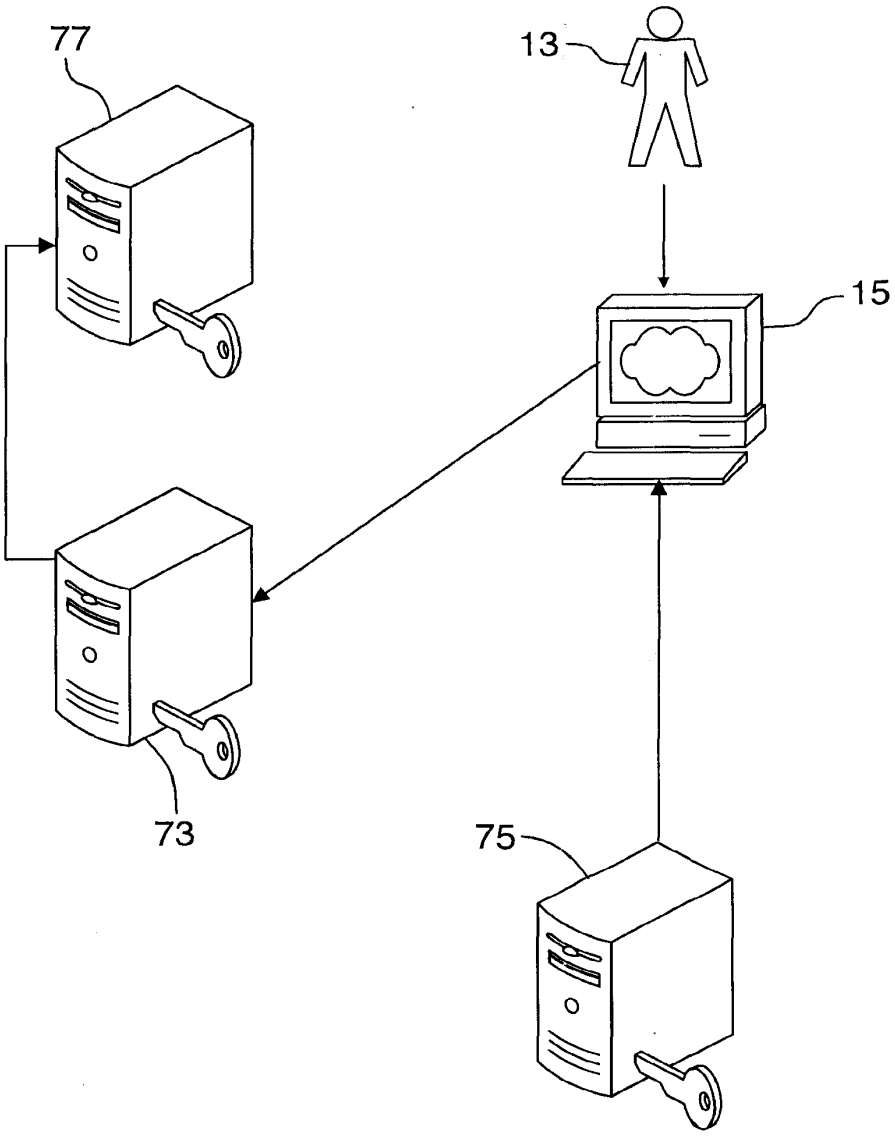


FIG.10

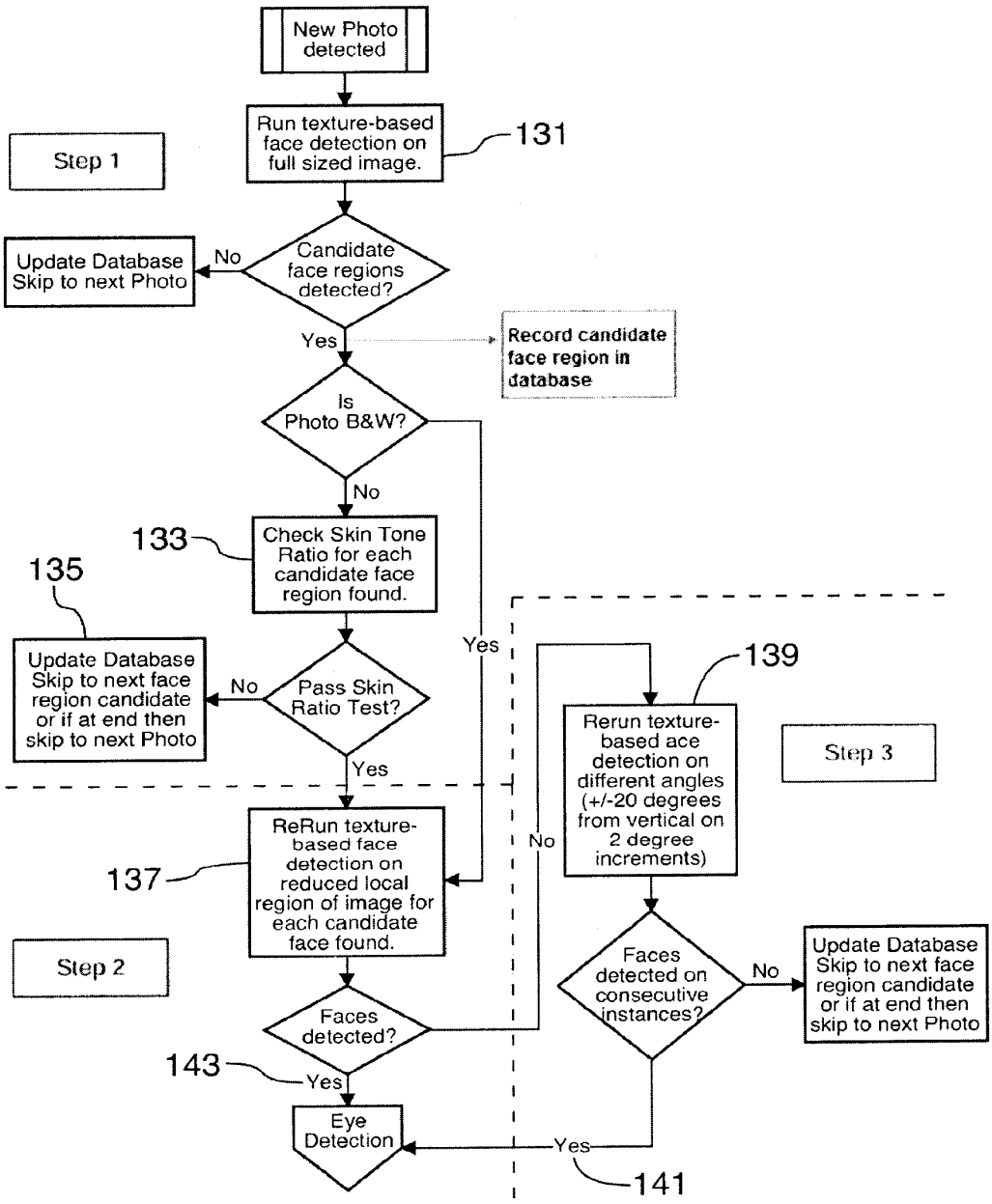

New Photo detected
Run texture-based face detection on full sized image.
131
Step 1
Update Database Skip to next Photo
No
Candidate face regions detected?
Yes
Record candidate face region in database
Is Photo B&W?
No
Yes
133
Check Skin Tone Ratio for each candidate face region found.
135
Update Database Skip to next face region candidate or if at end then skip to next Photo
No
Pass Skin Ratio Test?
Yes
139
Rerun texture-based ace detection on different angles (+/-20 degrees from vertical on 2 degree increments)
Step 3
No
137
ReRun texture-based face detection on reduced local region of image for each candidate face found.
Step 2
Faces detected on consecutive instances?
No
Update Database Skip to next face region candidate or if at end then skip to next Photo
Faces detected?
143
Yes
Eye Detection
Yes
141

FIG.11

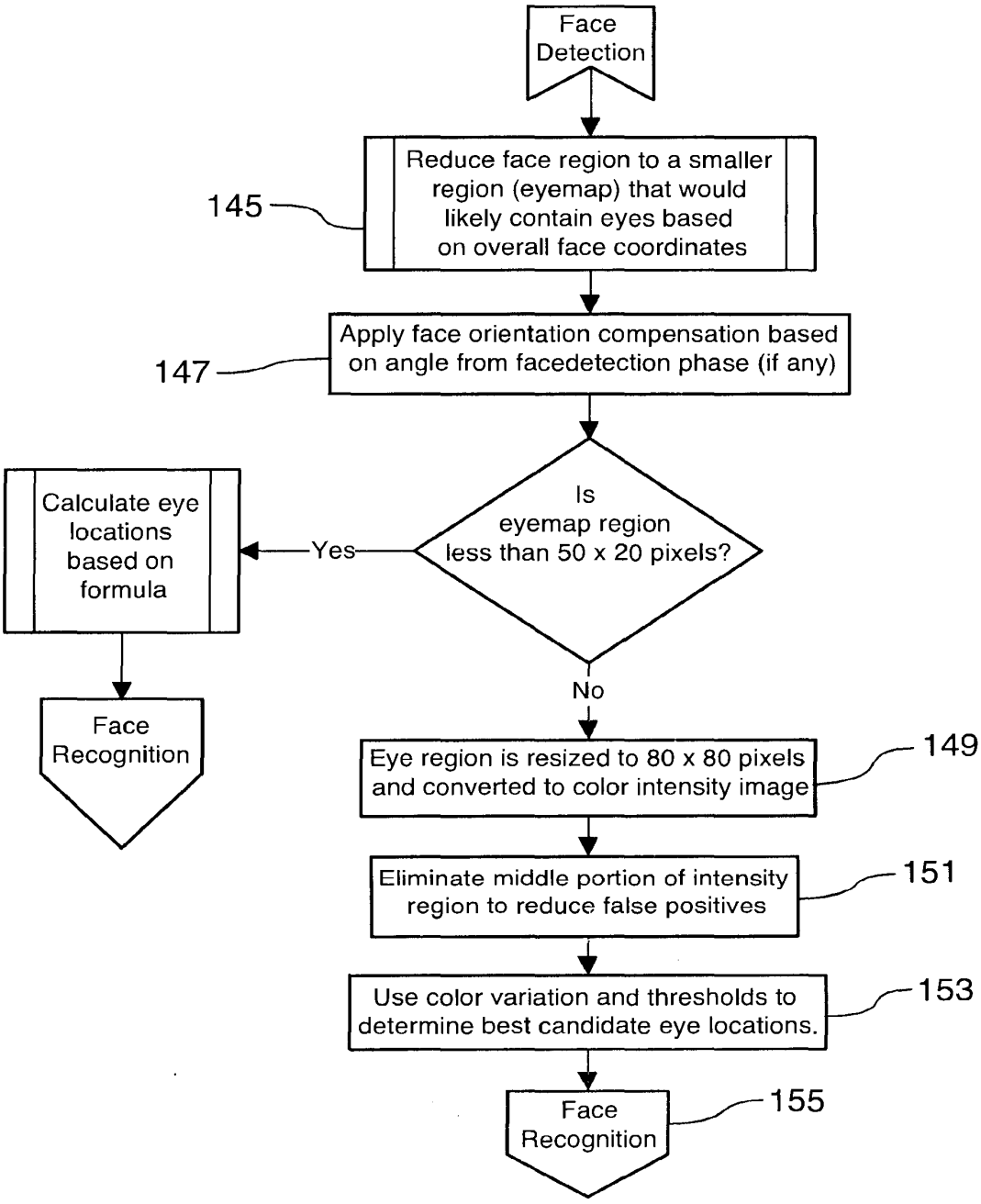

Face Detection
Reduce face region to a smaller region (eyemap) that would likely contain eyes based on overall face coordinates
145
Apply face orientation compensation based on angle from facedetection phase (if any)
147
Is eyemap region less than 50 x 20 pixels?
Yes
Calculate eye locations based on formula
Face Recognition
No
Eye region is resized to 80 x 80 pixels and converted to color intensity image
149
Eliminate middle portion of intensity region to reduce false positives
151
Use color variation and thresholds to determine best candidate eye locations.
153
Face Recognition
155

FIG.12

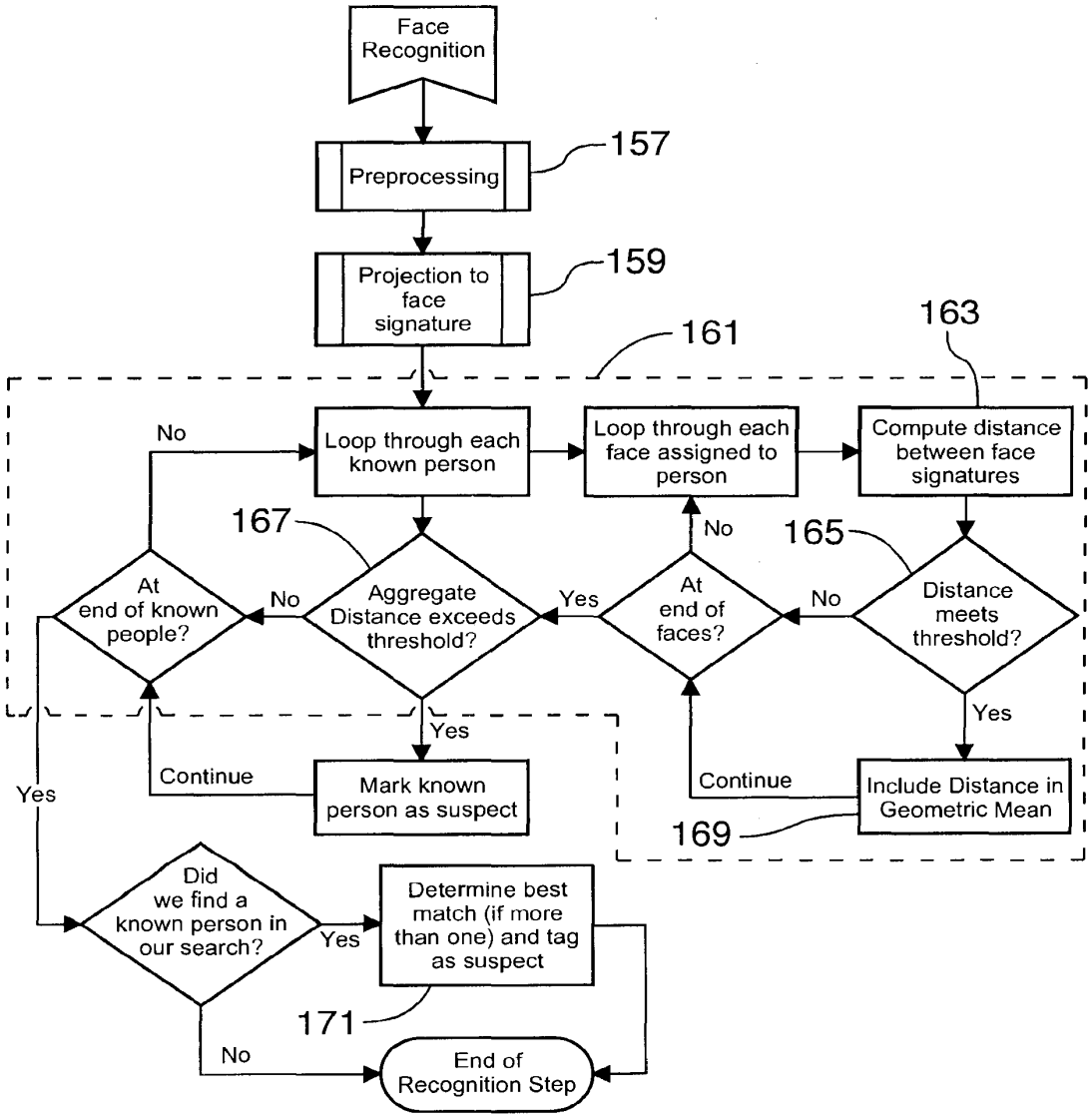

Face Recognition
Preprocessing
157
Projection to face signature
159
161
163
Loop through each known person
Loop through each face assigned to person
Compute distance between face signatures
No
No
No
167
165
At end of known people?
Aggregate Distance exceeds threshold?
At end of faces?
Distance meets threshold?
Yes
Yes
Yes
Yes
Continue
Continue
Mark known person as suspect
Include Distance in Geometric Mean
169
Did we find a known person in our search?
Yes
Determine best match (if more than one) and tag as suspect
171
No
End of Recognition Step

FIG.13

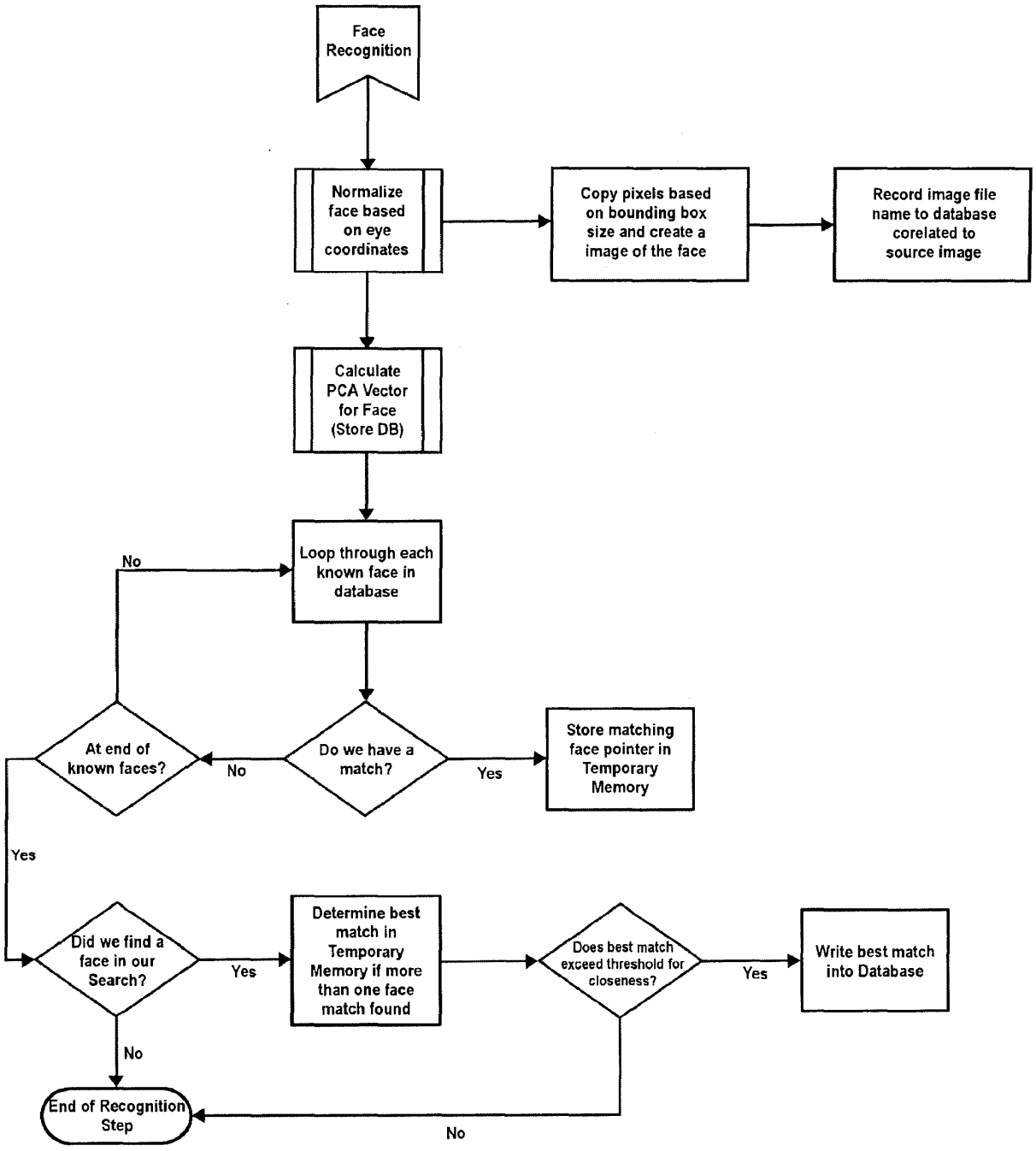

Face Recognition
Normalize face based on eye coordinates
Copy pixels based on bounding box size and create a image of the face
Record image file name to database corelated to source image
Calculate PCA Vector for Face (Store DB)
Loop through each known face in database
No
At end of known faces?
No
Do we have a match?
Yes
Store matching face pointer in Temporary Memory
Yes
Did we find a face in our Search?
Yes
Determine best match in Temporary Memory if more than one face match found
Does best match exceed threshold for closeness?
Yes
Write best match into Database
No
End of Recognition Step
No

FIG. 13A

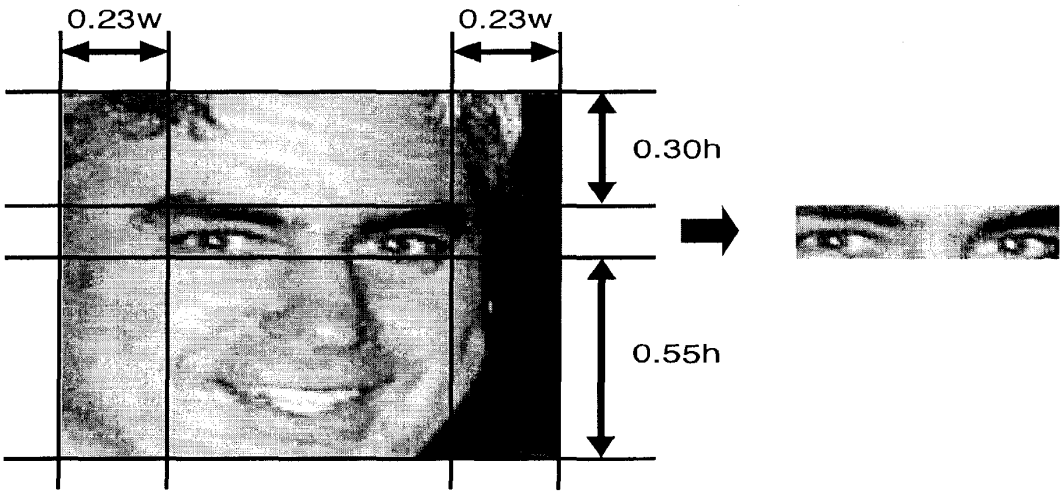


FIG.14A

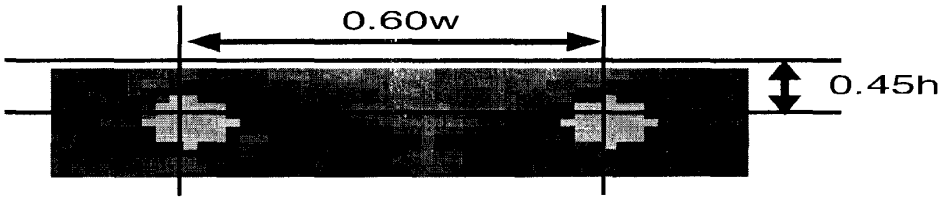


FIG.14B

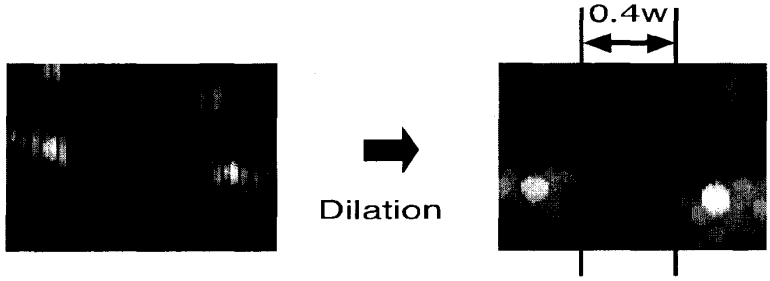


FIG.14C

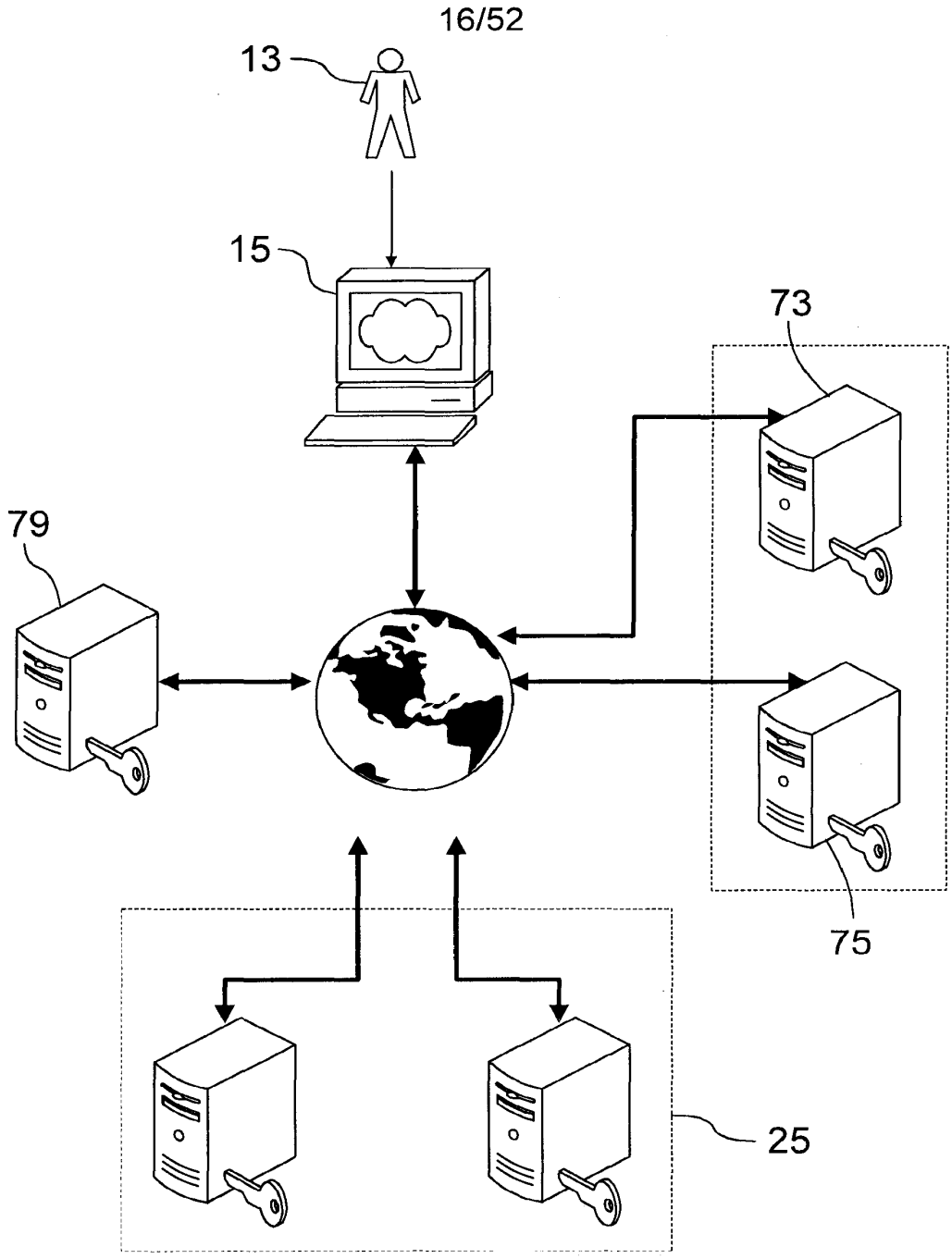


FIG.15

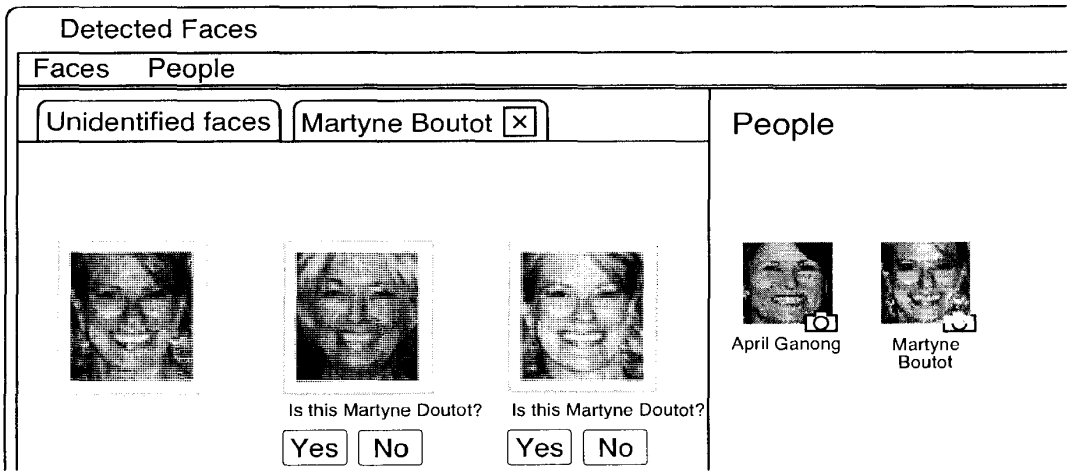

Detected Faces
Faces People
Unidentified faces
Martyne Boutot
People
Is this Martyne Doutot?
Yes
No
Is this Martyne Doutot?
Yes
No
April Ganong
Martyne Boutot

FIG.16

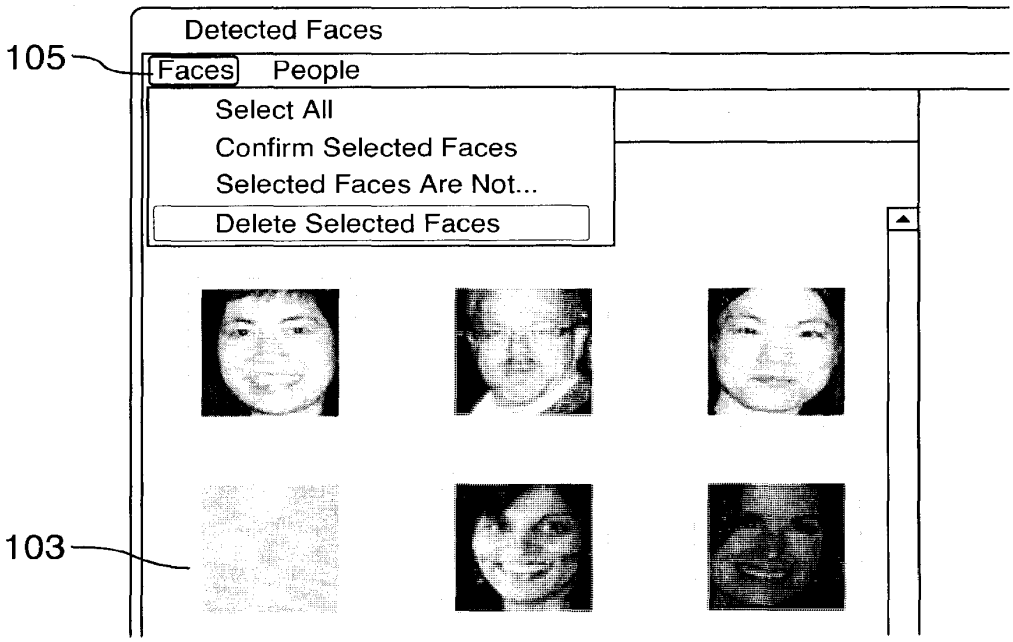

105
Detected Faces
Faces
People
Select All
Confirm Selected Faces
Selected Faces Are Not...
Delete Selected Faces
103

FIG.17

Adjust Eye Coordinates
107
109

FIG.18

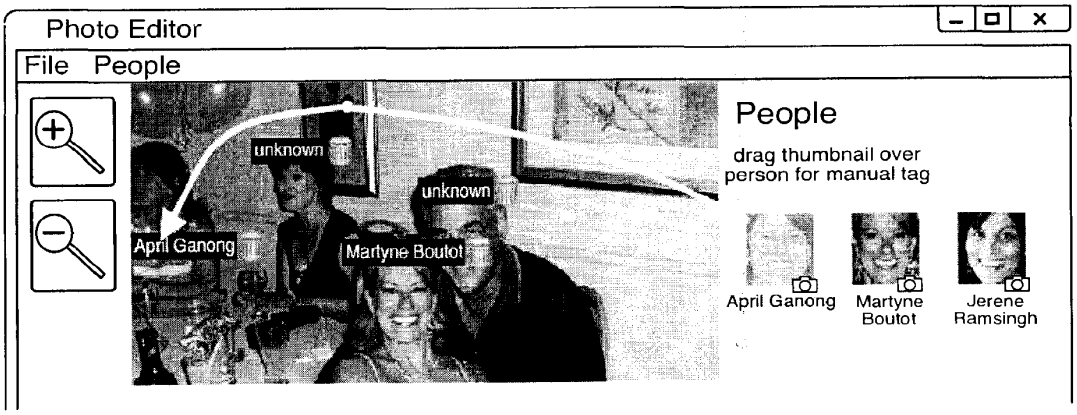


Photo Editor
File People
unknown
unknown
April Ganong
Martyne Boutot
People
drag thumbnail over person for manual tag
April Ganong
Martyne Boutot
Jerene Ramsingh

FIG.19

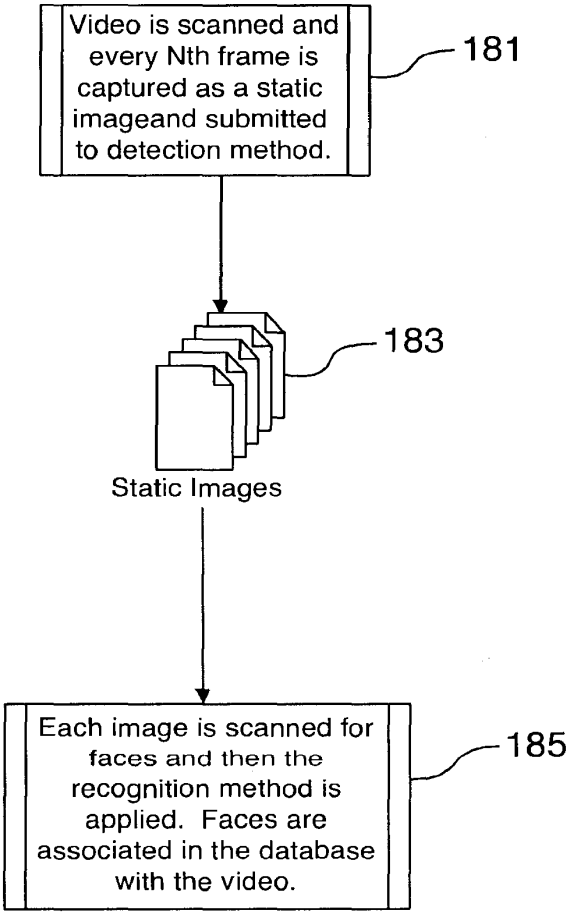

Video is scanned and every Nth frame is captured as a static imageand submitted to detection method.
181
183
Static Images
Each image is scanned for faces and then the recognition method is applied. Faces are associated in the database with the video.
185

FIG.20

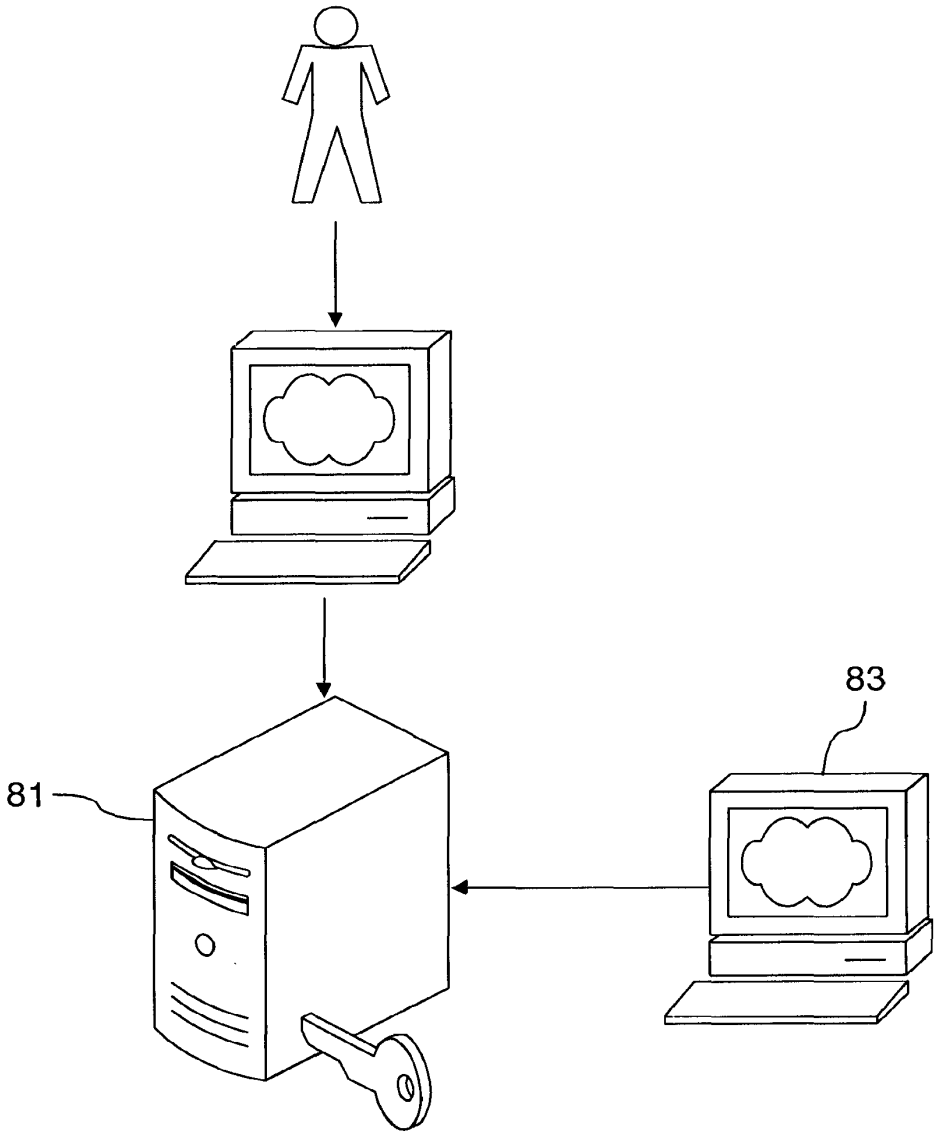


FIG.21

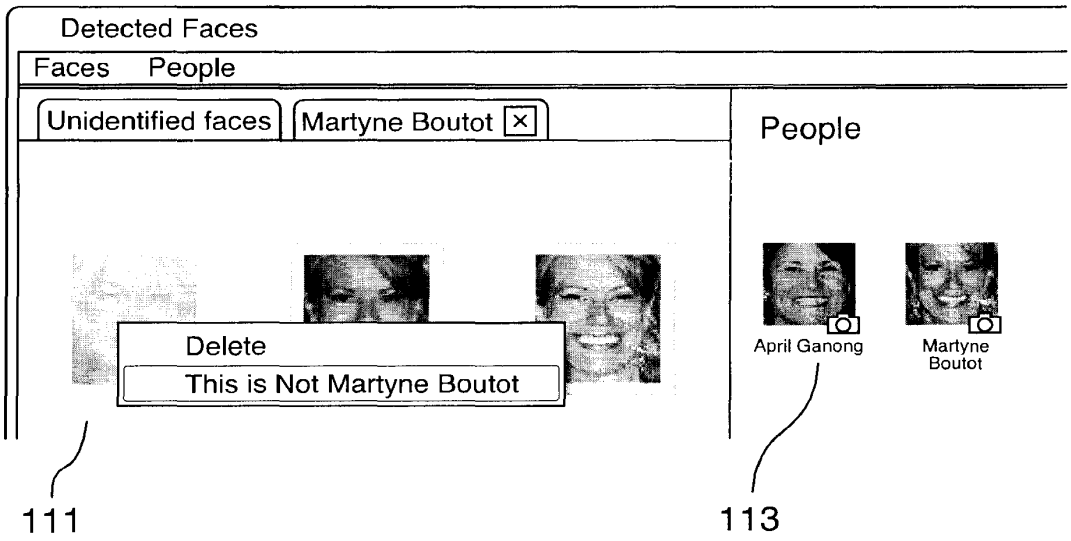

Detected Faces
Faces People
Unidentified faces
Martyne Boutot
People
Delete
This is Not Martyne Boutot
April Ganong
Martyne Boutot
111
113

FIG.22

Figure 23

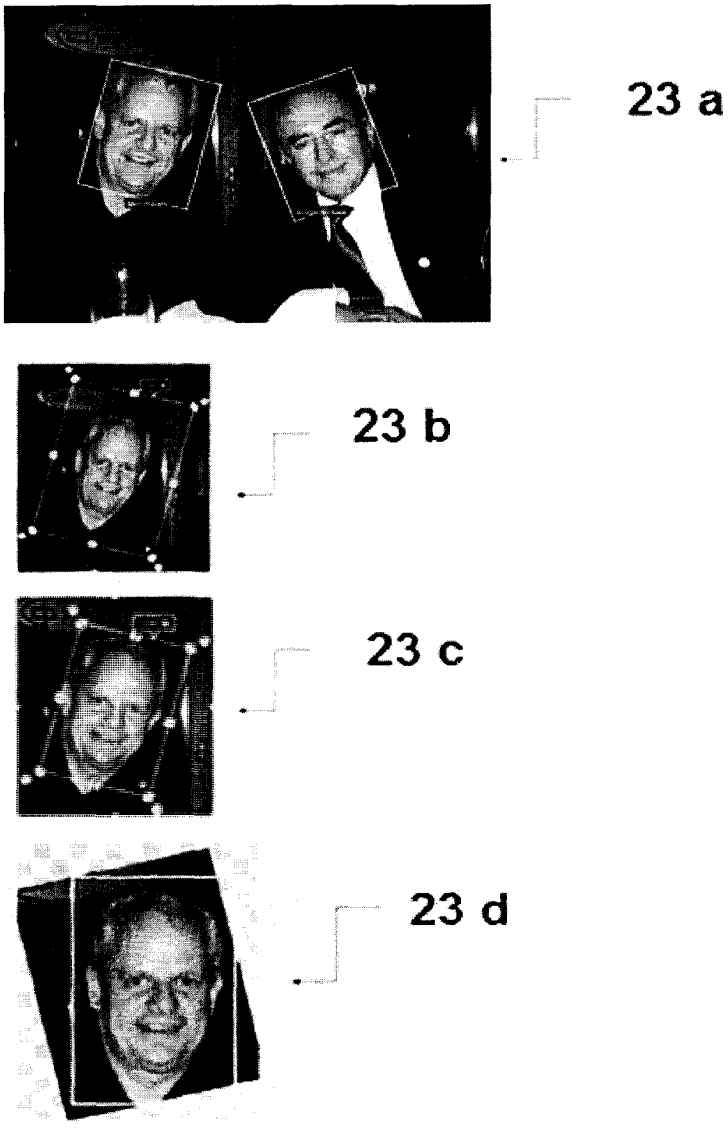
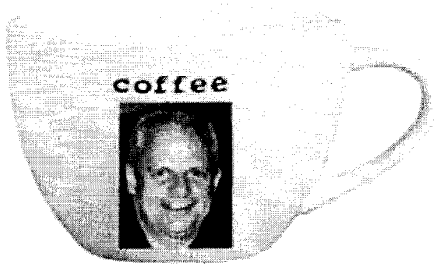


Figure 24

24 a

24 b



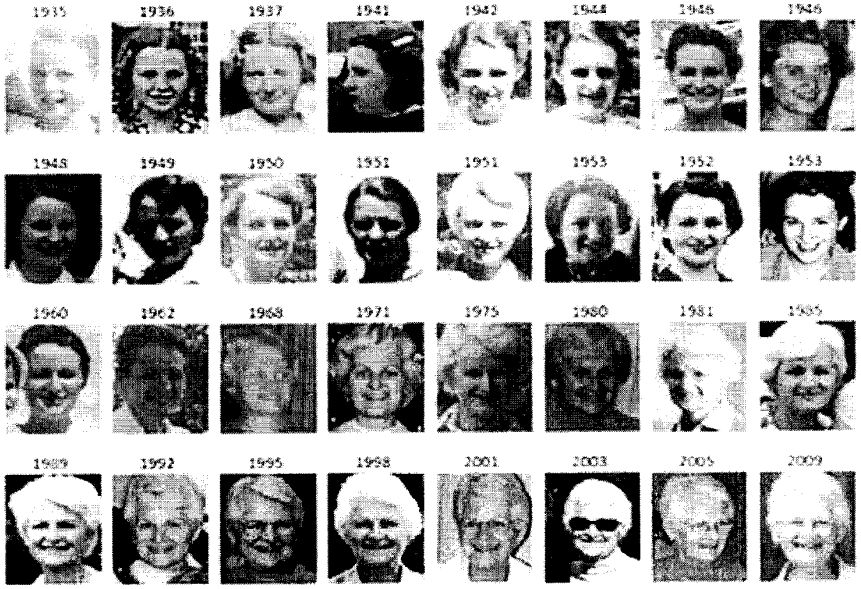
24 c

Figure 25

25 a

25 b

Figure 26



26 a

26 b

Figure 27

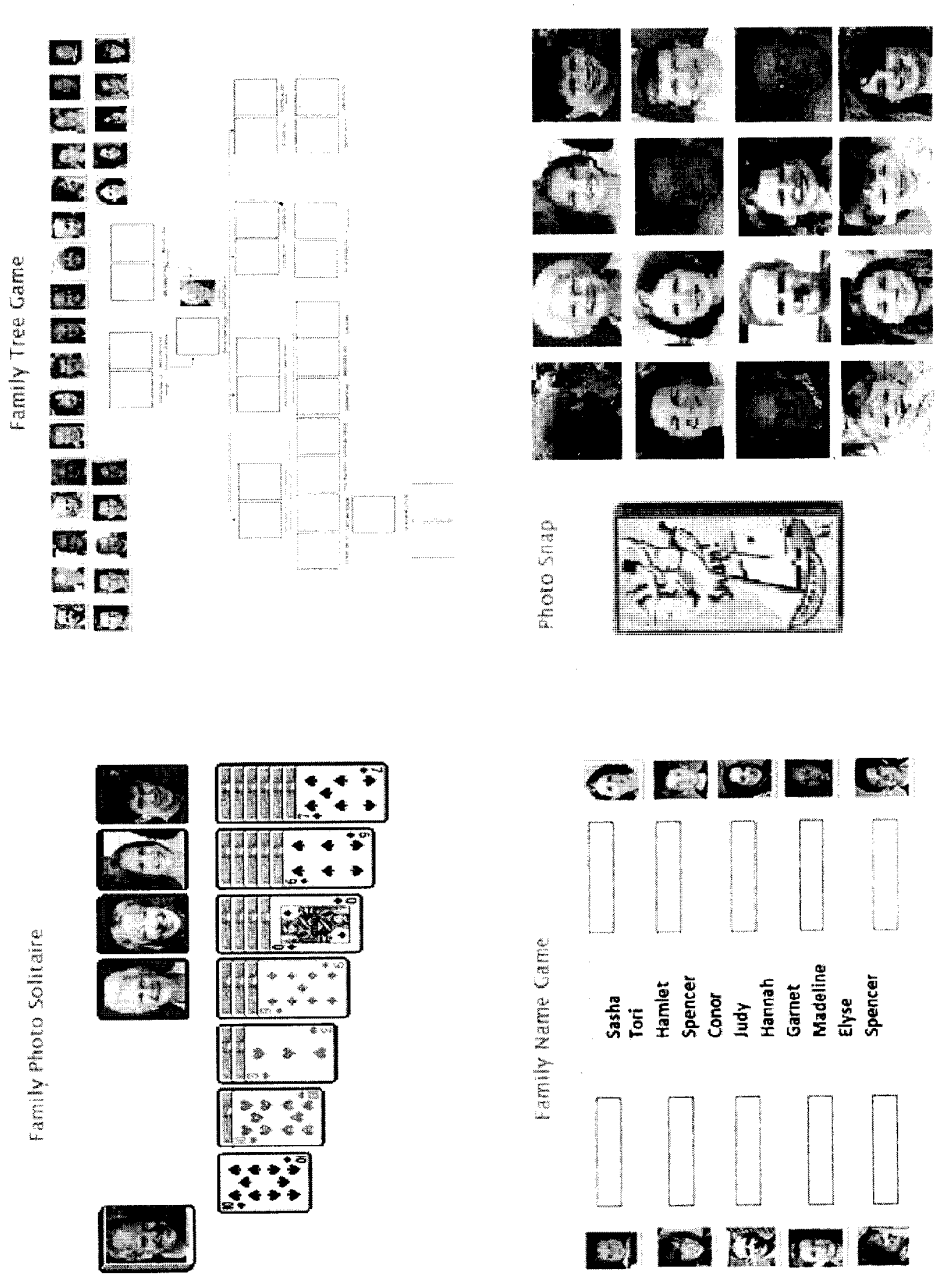

Family Tree Game
Photo Snap
Family Photo Solitaire
Family Name Game
Sasha
Tori
Hamlet
Spencer
Conor
Judy
Hannah
Garnet
Madeline
Elyse
Spencer

Figure 28

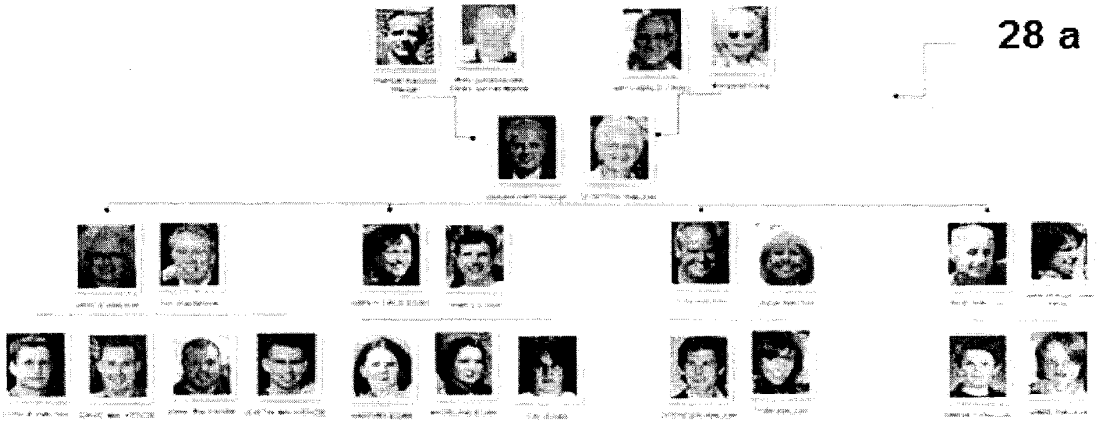


Figure 29

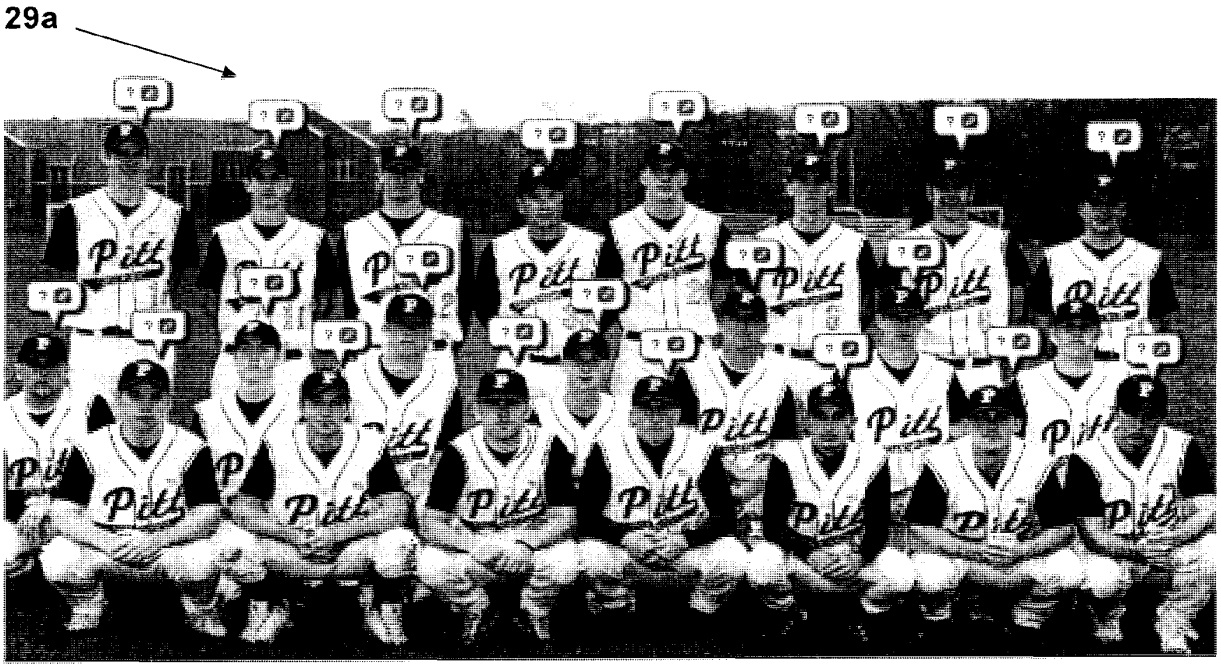


Figure 30

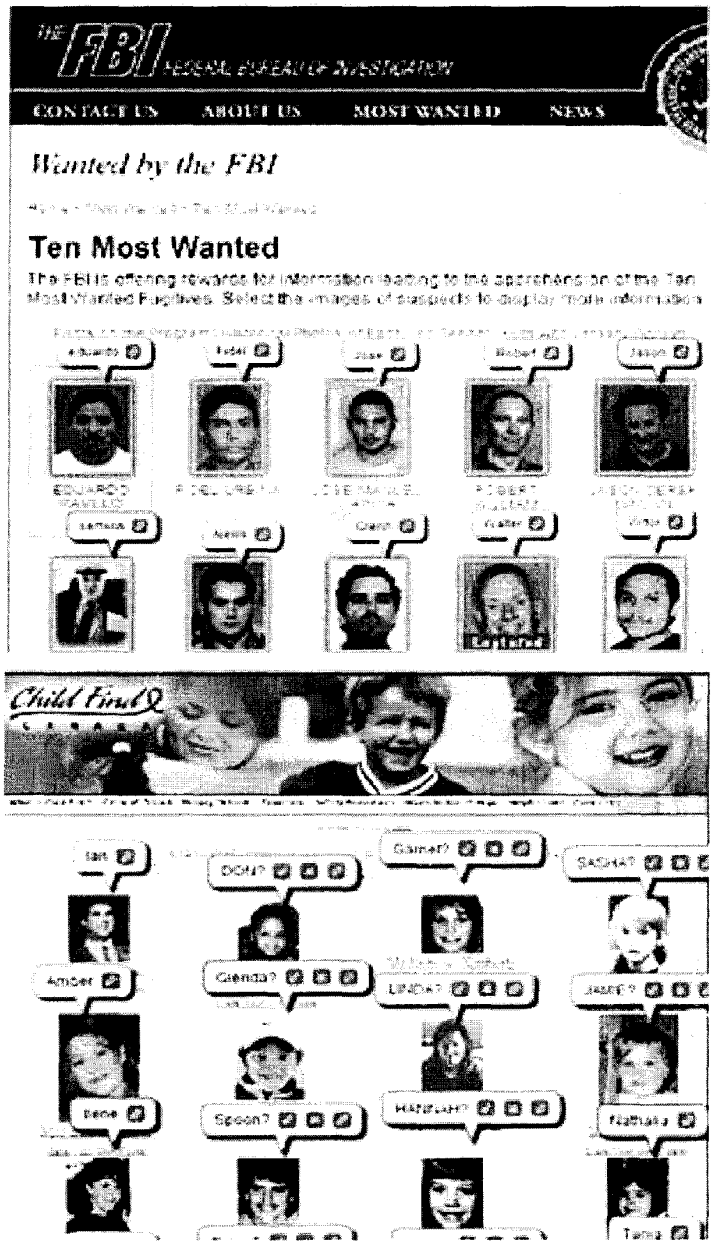

CONTACT US
ABOUT US
MOST WANTED
NEWS
Wanted by the FBI
Ten Most Wanted
Child Find
30 a
30 b

Figure 31

Figure 32

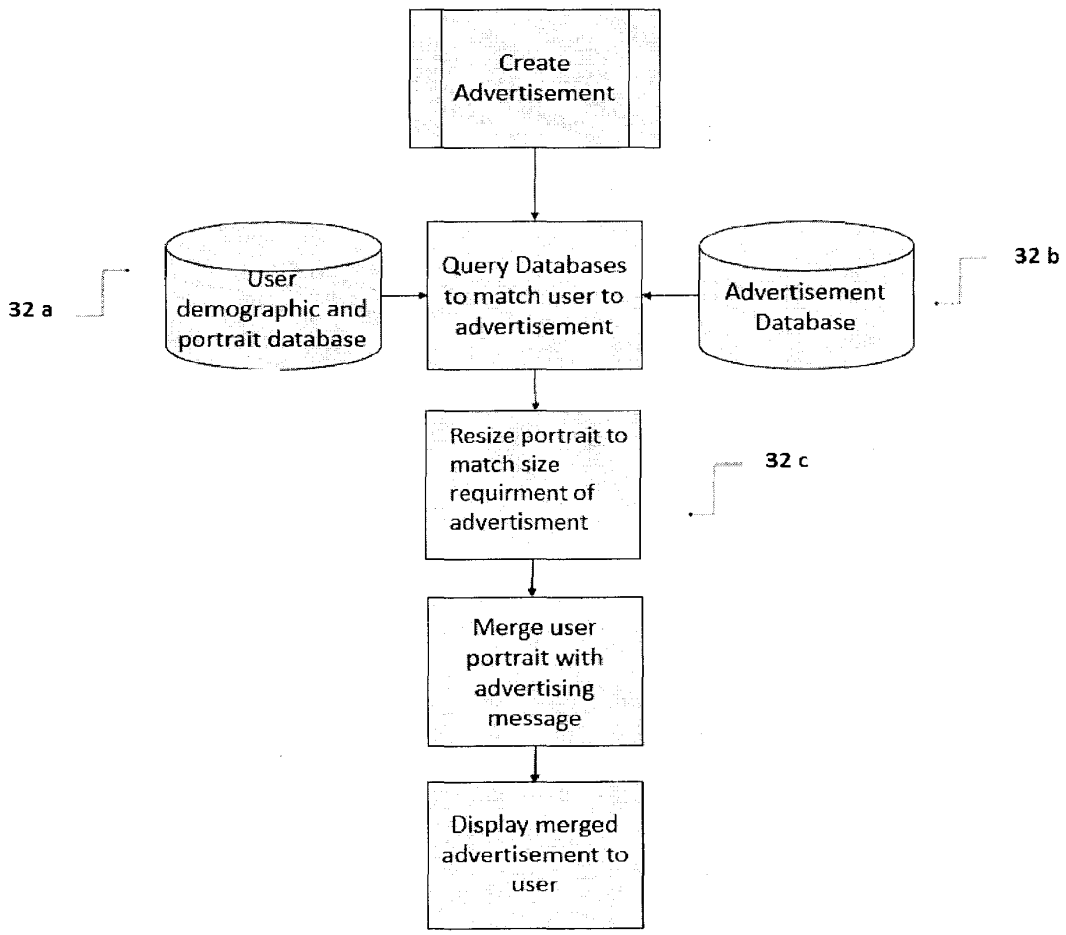

Create Advertisement
User demographic and portrait database
Query Databases to match user to advertisement
Advertisement Database
32 a
32 b
Resize portrait to match size requirment of advertisment
32 c
Merge user portrait with advertising message
Display merged advertisement to user

Figure 33

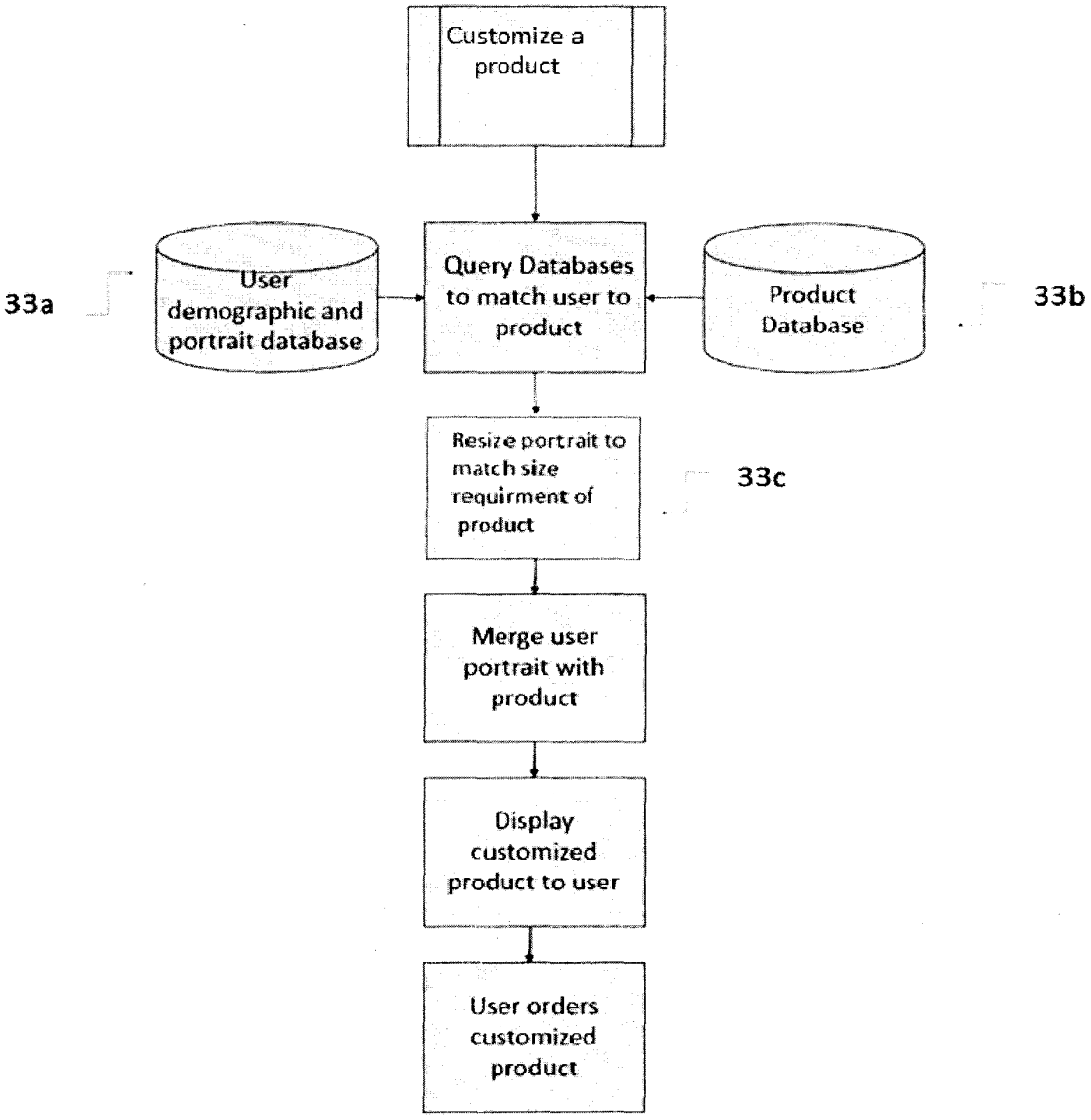

Customize a product
Query Databases to match user to product
User demographic and portrait database
33a
Product Database
33b
Resize portrait to match size requirment of product
33c
Merge user portrait with product
Display customized product to user
User orders customized product

Figure 34

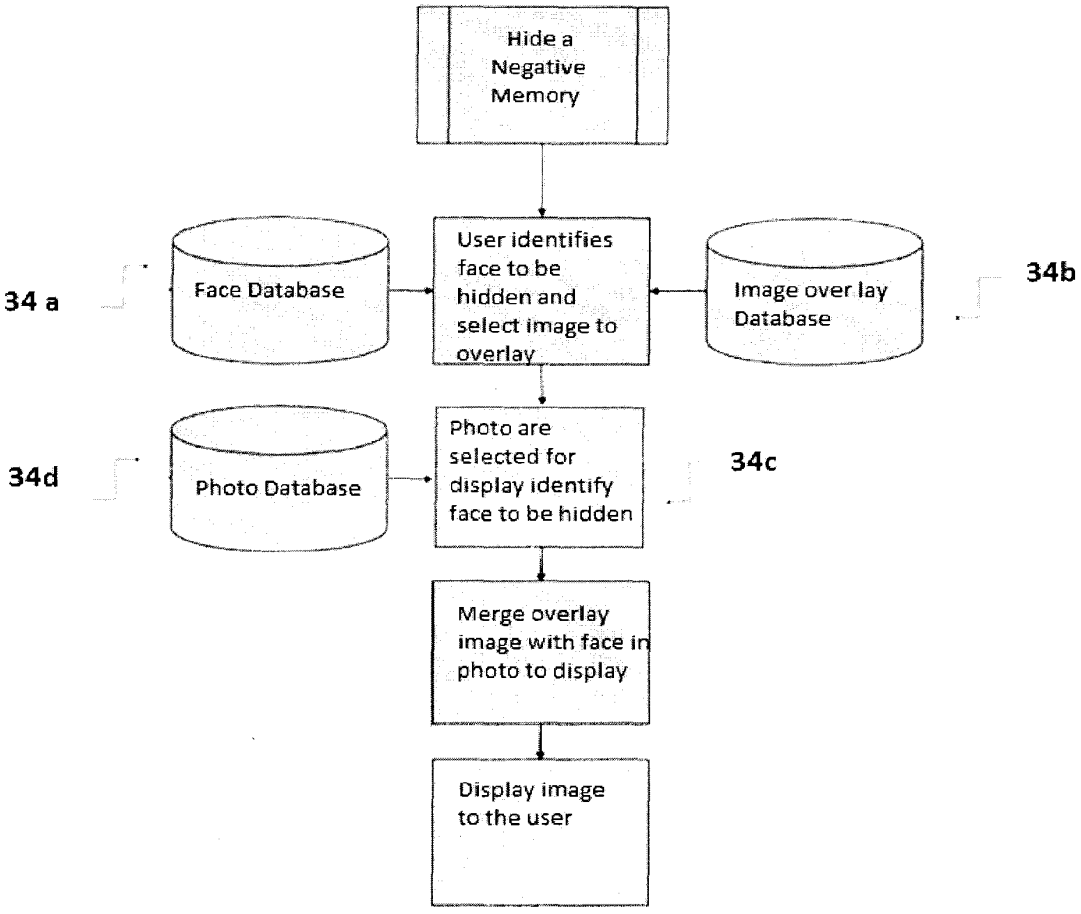

Hide a Negative Memory
User identifies face to be hidden and select image to overlay
Face Database
Image over lay Database
Photo Database
Photo are selected for display identify face to be hidden
Merge overlay image with face in photo to display
Display image to the user
34 a
34b
34c
34d

Figure 35

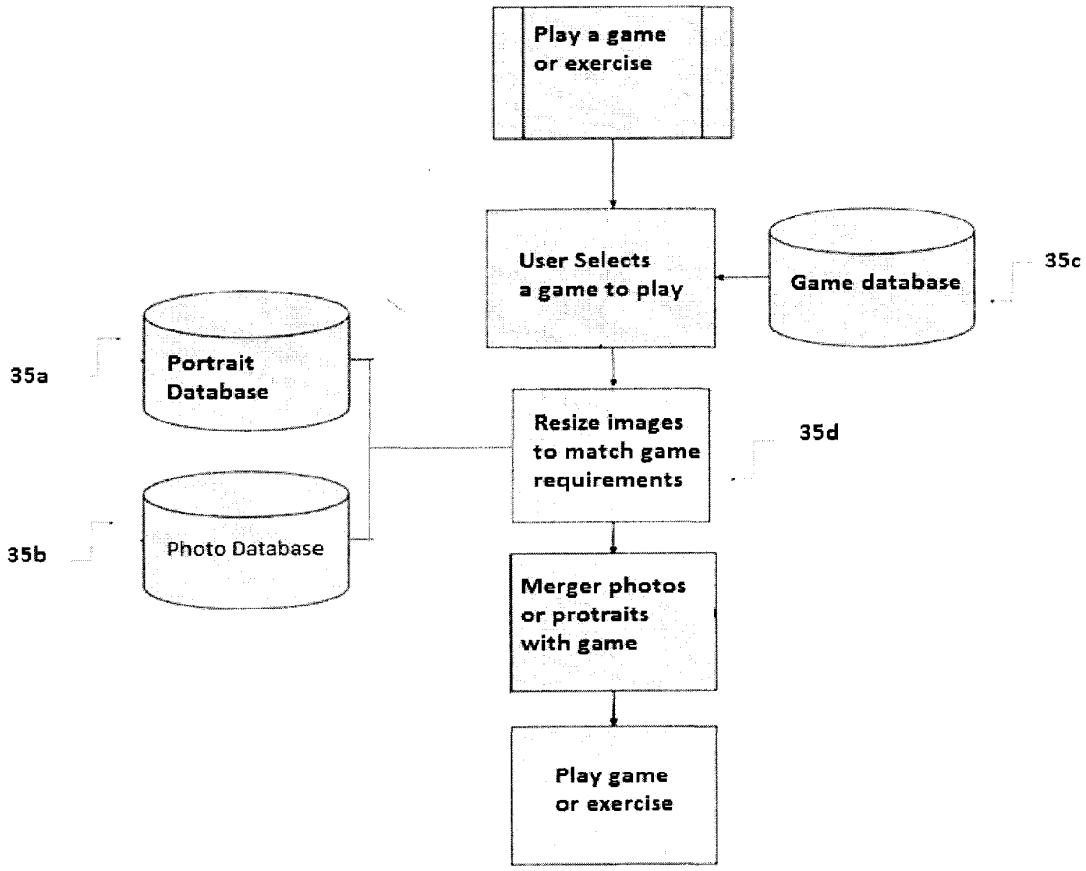

Play a game or exercise
User Selects a game to play
Game database
35c
Portrait Database
35a
Resize images to match game requirements
35d
Photo Database
35b
Merger photos or protraits with game
Play game or exercise

Figure 36

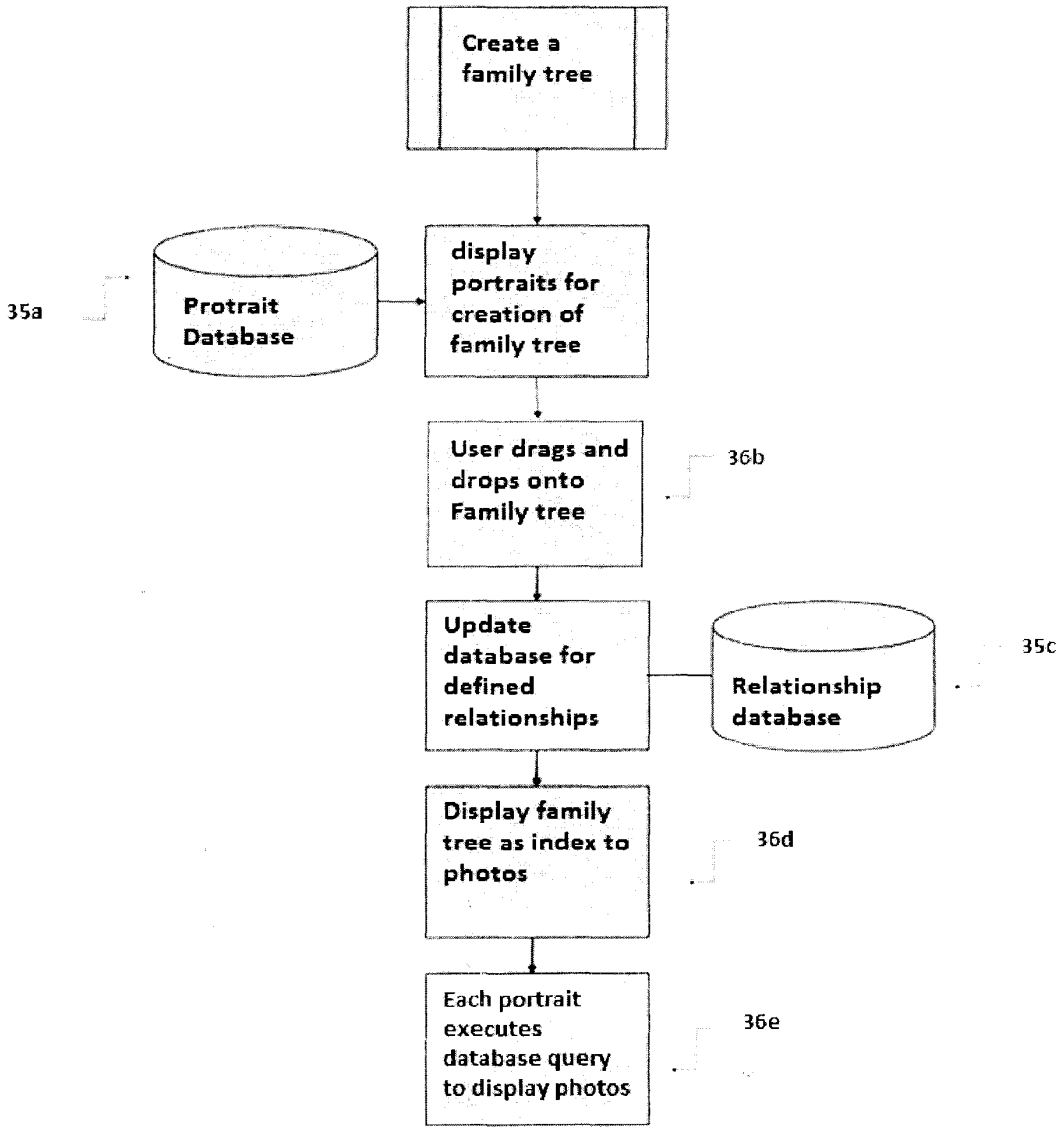

Create a family tree
display portraits for creation of family tree
Protrait Database
35a
User drags and drops onto Family tree
36b
Update database for defined relationships
Relationship database
35c
Display family tree as index to photos
36d
Each portrait executes database query to display photos
36e

Figure 37

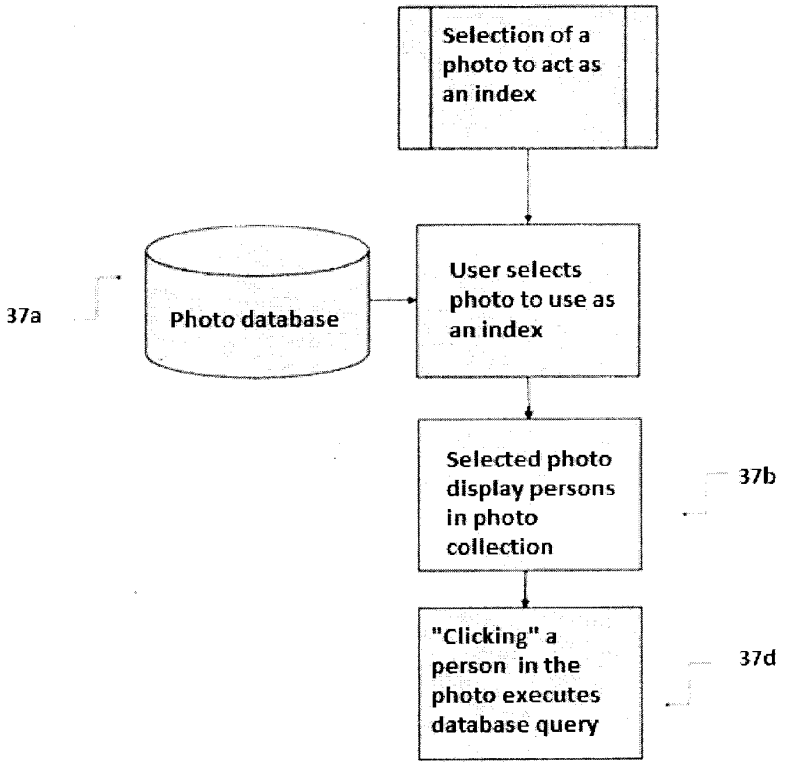

Selection of a photo to act as an index
User selects photo to use as an index
Photo database
37a
Selected photo display persons in photo collection
37b
"Clicking" a person in the photo executes database query
37d

Figure 38

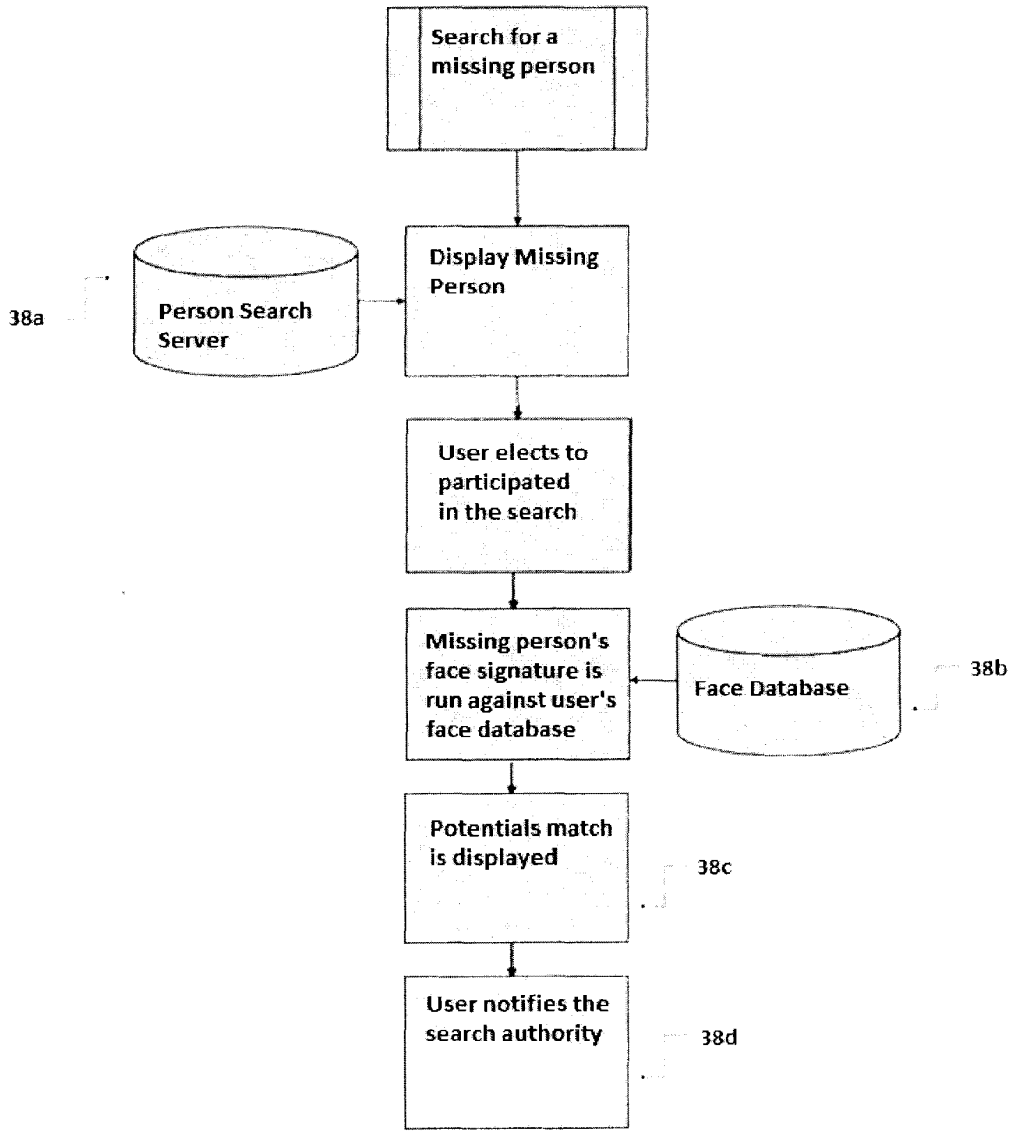

Search for a missing person
Display Missing Person
Person Search Server
38a
User elects to participated in the search
Missing person's face signature is run against user's face database
Face Database
38b
Potentials match is displayed
38c
User notifies the search authority
38d

Figure 39

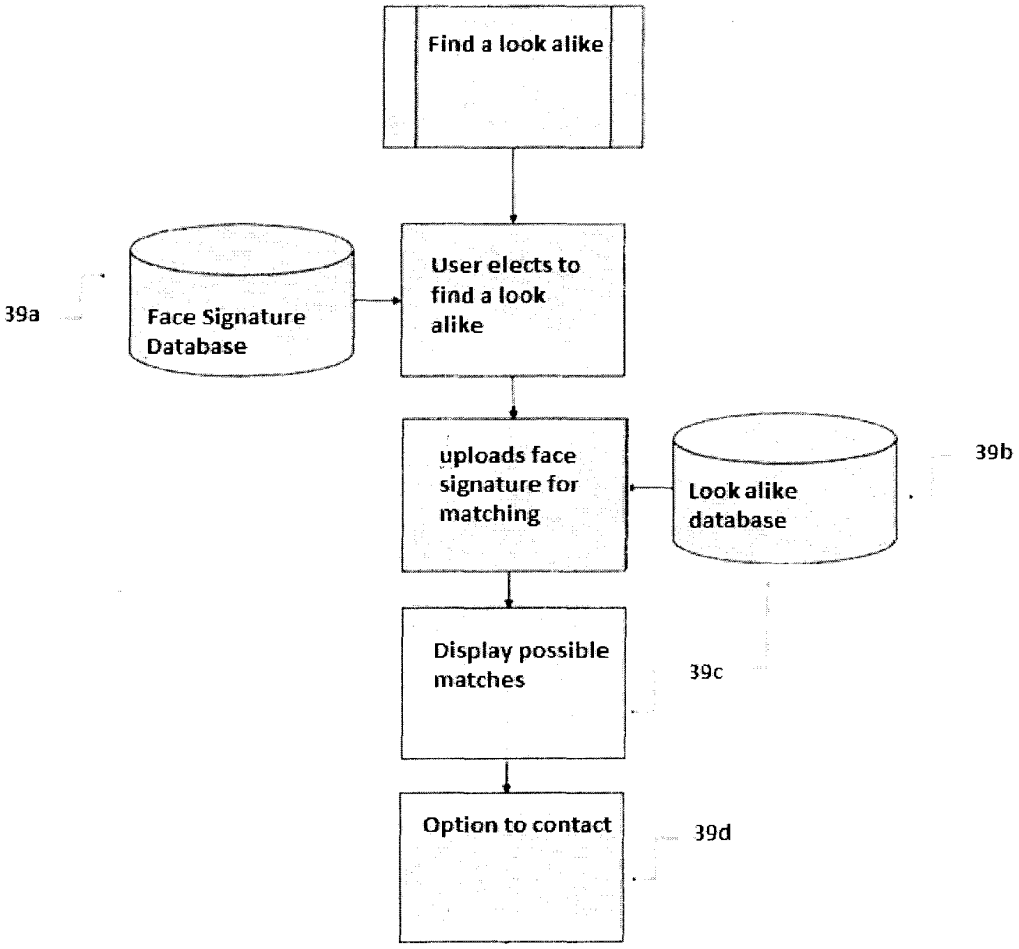

Find a look alike
User elects to find a look alike
39a
Face Signature Database
uploads face signature for matching
Look alike database
39b
Display possible matches
39c
Option to contact
39d

Figure 40 – Same Image

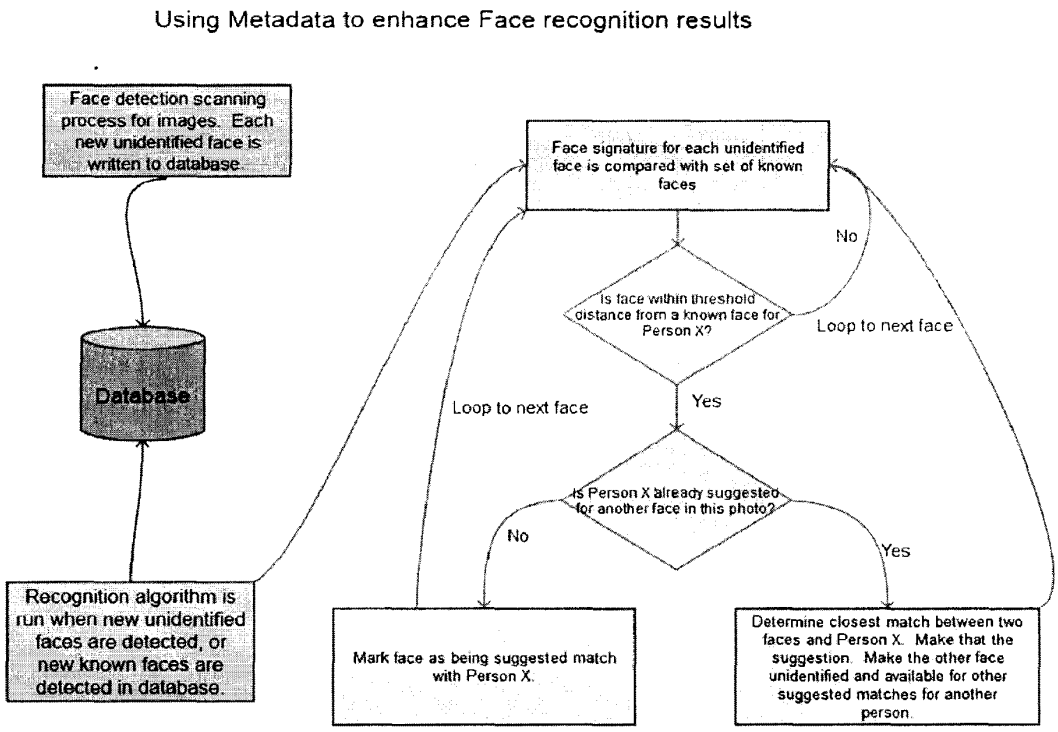


Figure 41 – Same Date

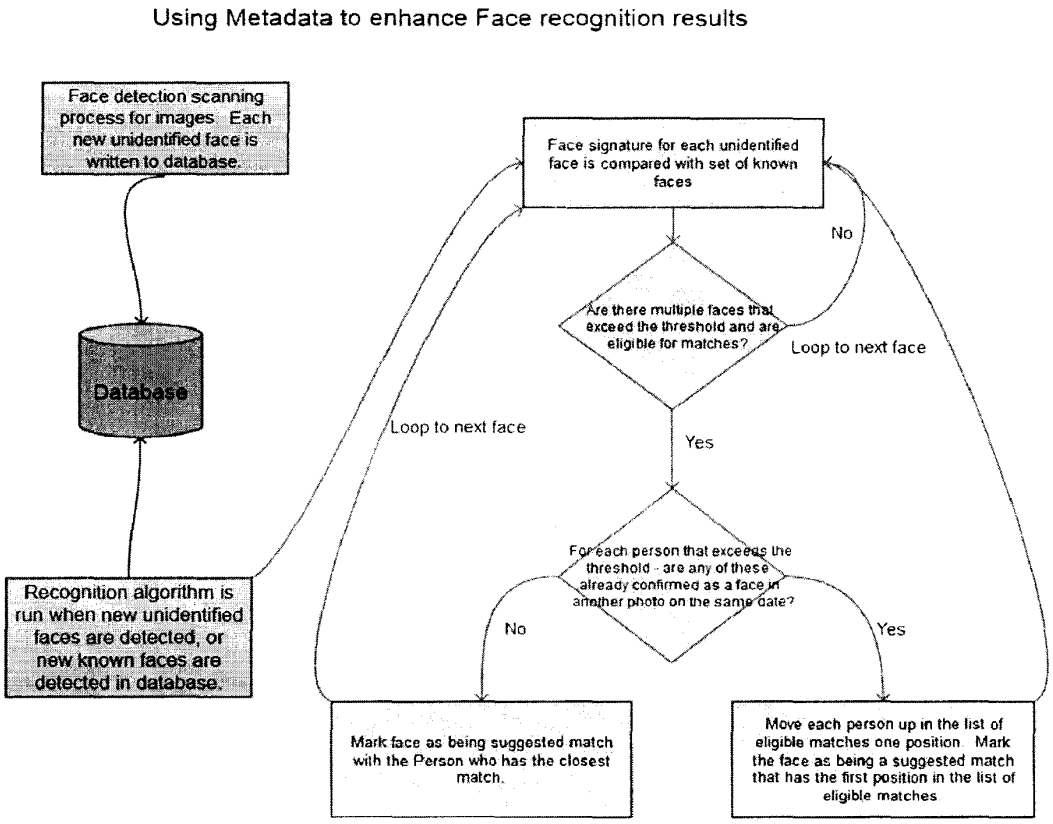


Figure 42 - Relationships

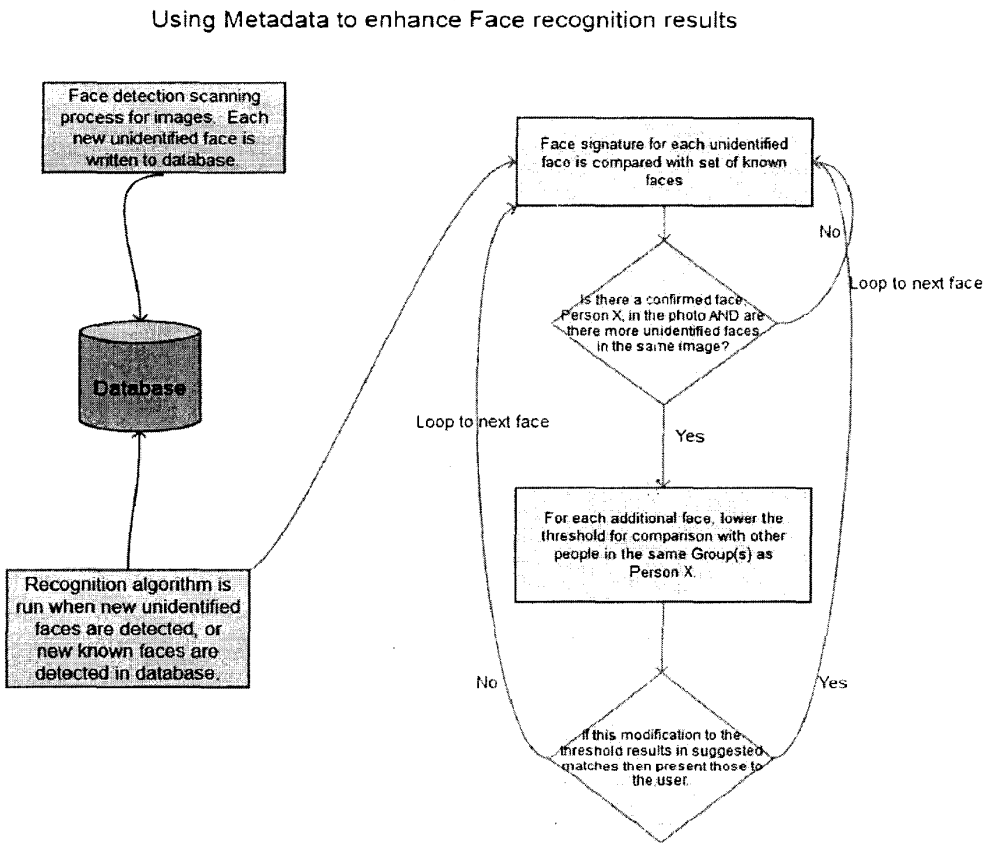


Figure 43 - Locations

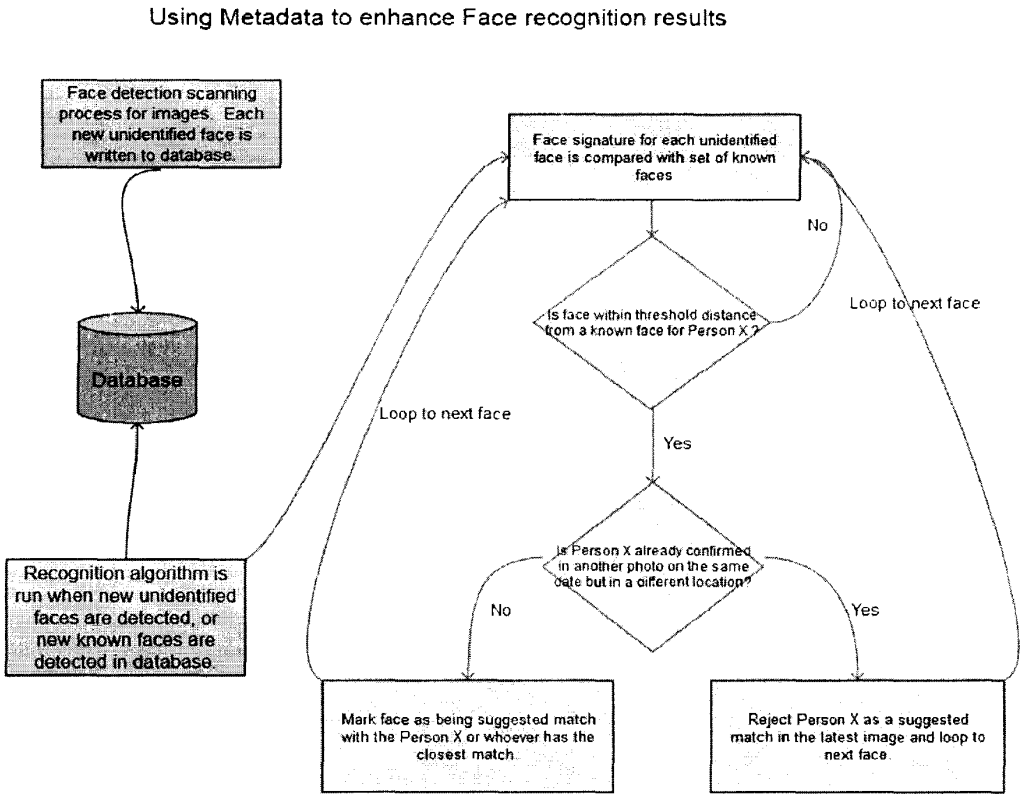


Figure 44 – Event Information

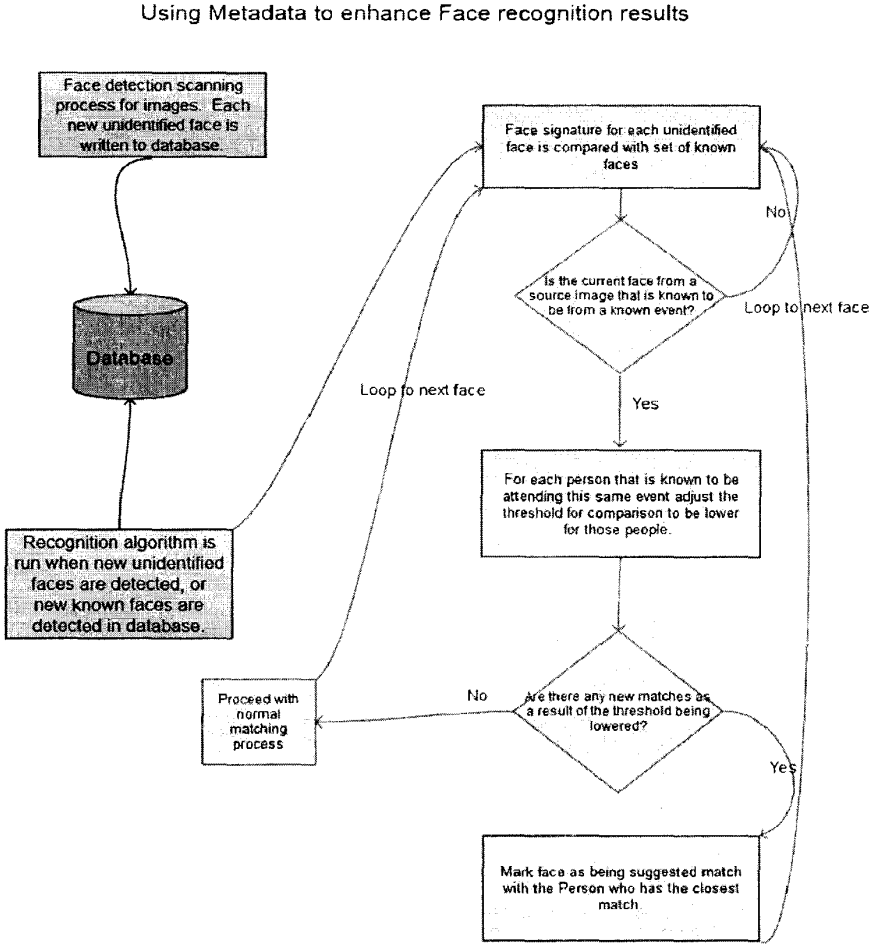


Figure 45 – Object Information

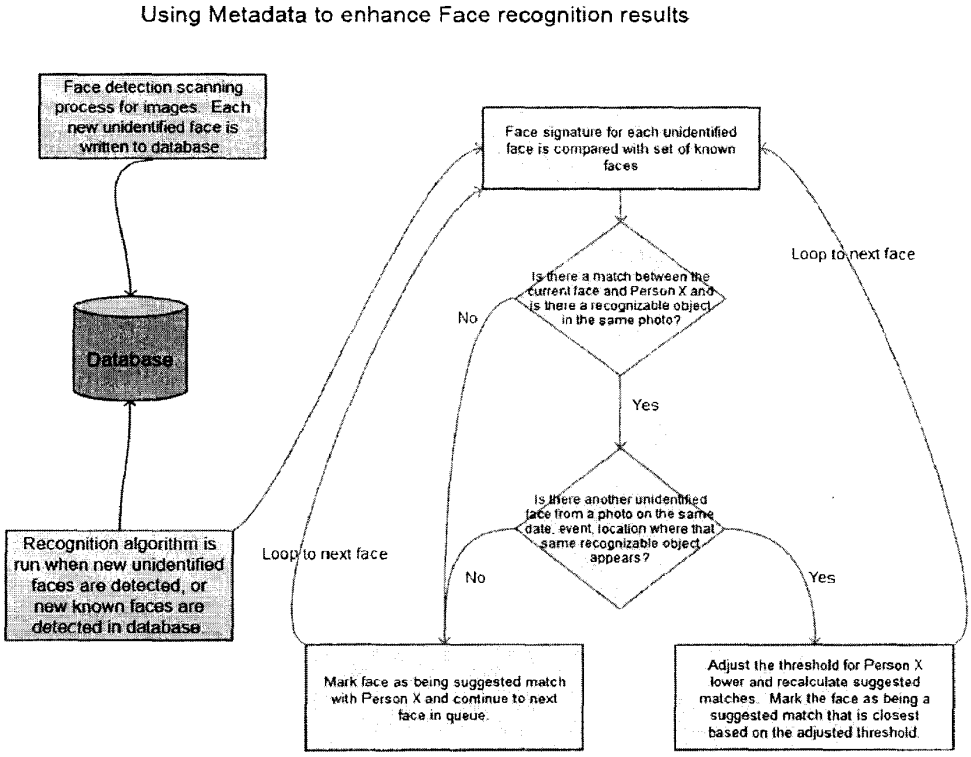


Figure 46

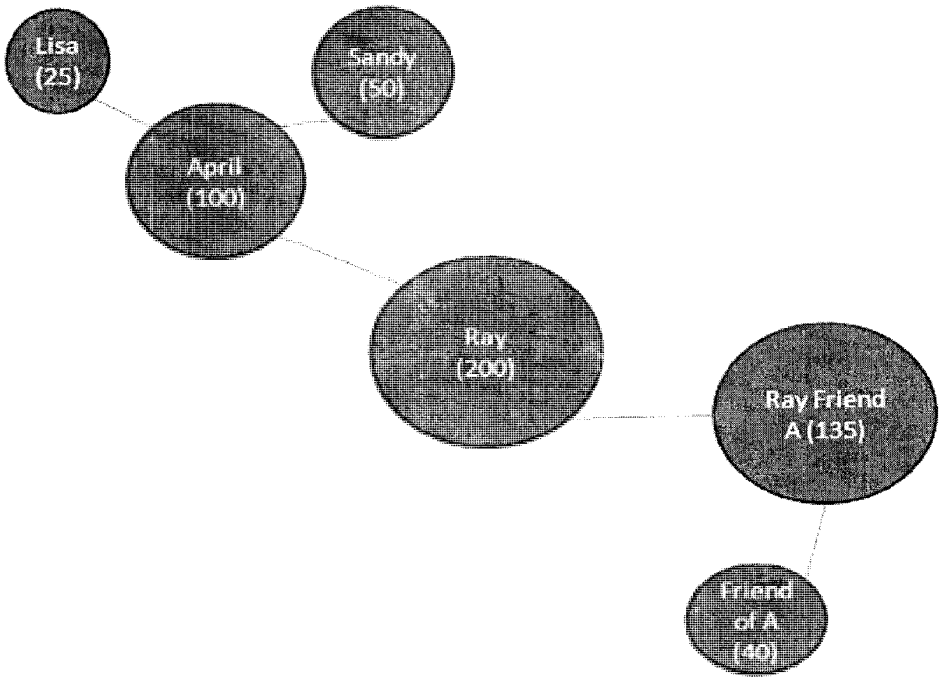

Lisa (25)
Sandy (50)
April (100)
Ray (200)
Ray Friend A (135)
Friend of A (40)

Figure 47

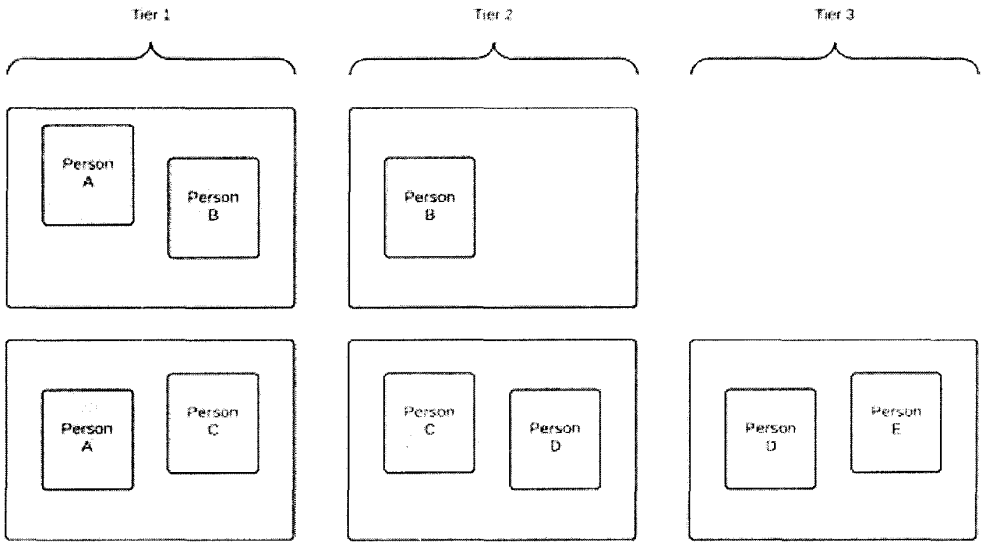

Tier 1
Tier 2
Tier 3
Person A
Person B
Person B
Person A
Person C
Person C
Person D
Person D
Person E

Figure 48

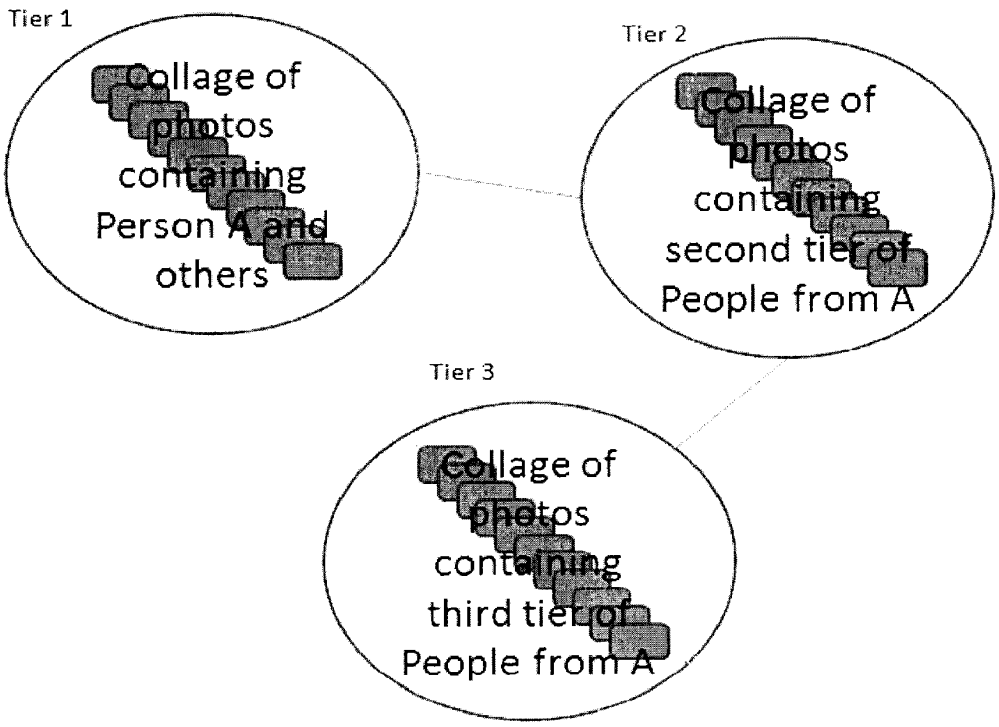

Tier 1
Collage of photos containing Person A and others
Tier 2
Collage of photos containing second tier of People from A
Tier 3
Collage of photos containing third tier of People from A

Figure 49

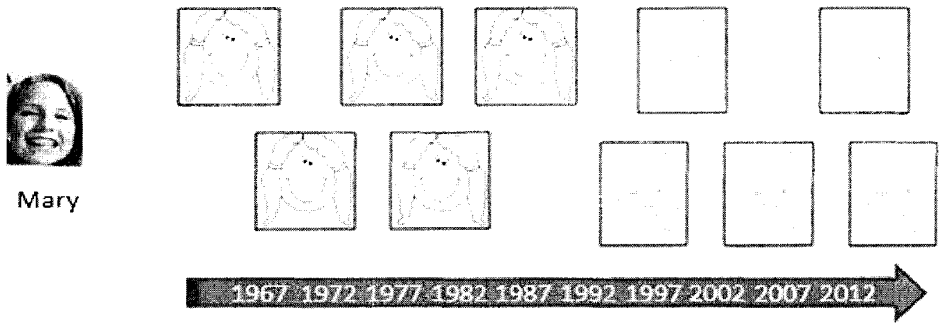


Figure 50

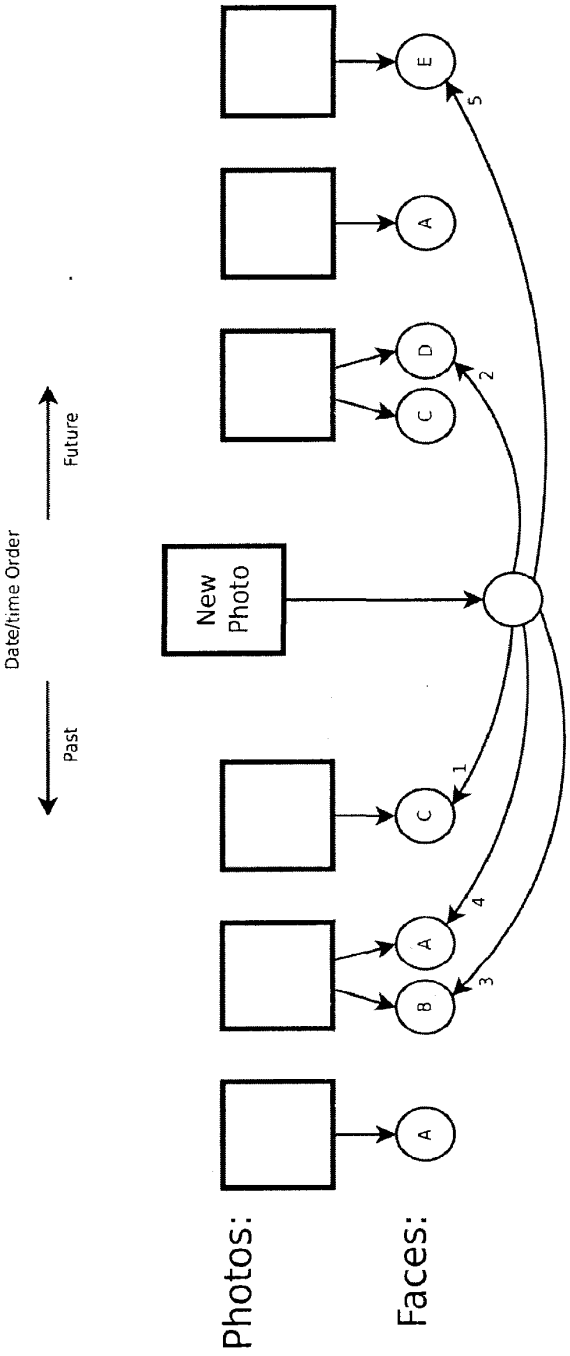

Photos:
Faces:
A
B
A
C
New Photo
C
D
A
E
1
2
3
4
5
Date/time Order
Future
Past

Figure 51

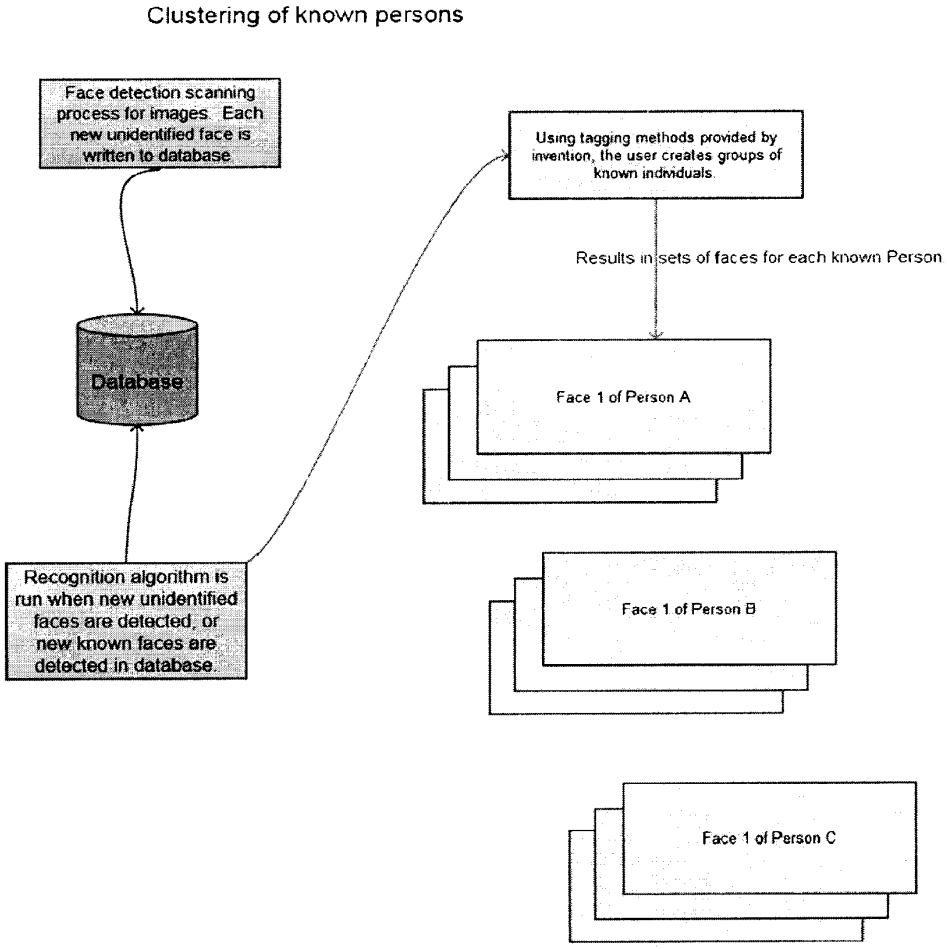

Clustering of known persons
Face detection scanning process for images. Each new unidentified face is written to database
Database
Recognition algorithm is run when new unidentified faces are detected, or new known faces are detected in database.
Using tagging methods provided by invention, the user creates groups of known individuals.
Results in sets of faces for each known Person
Face 1 of Person A
Face 1 of Person B
Face 1 of Person C

Figure 52

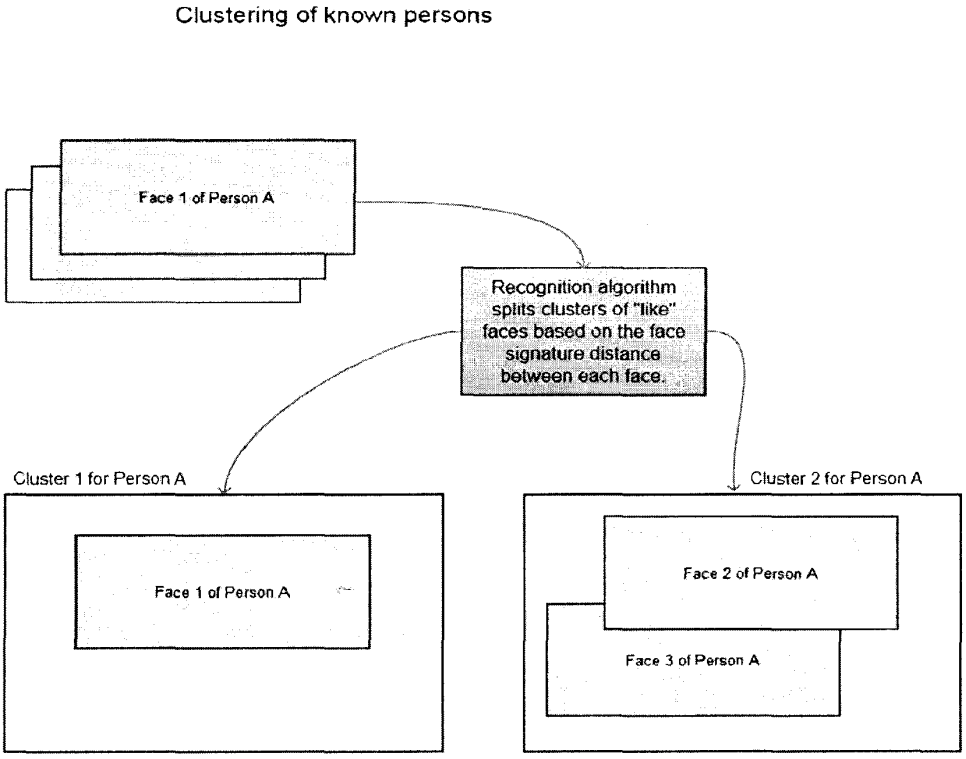
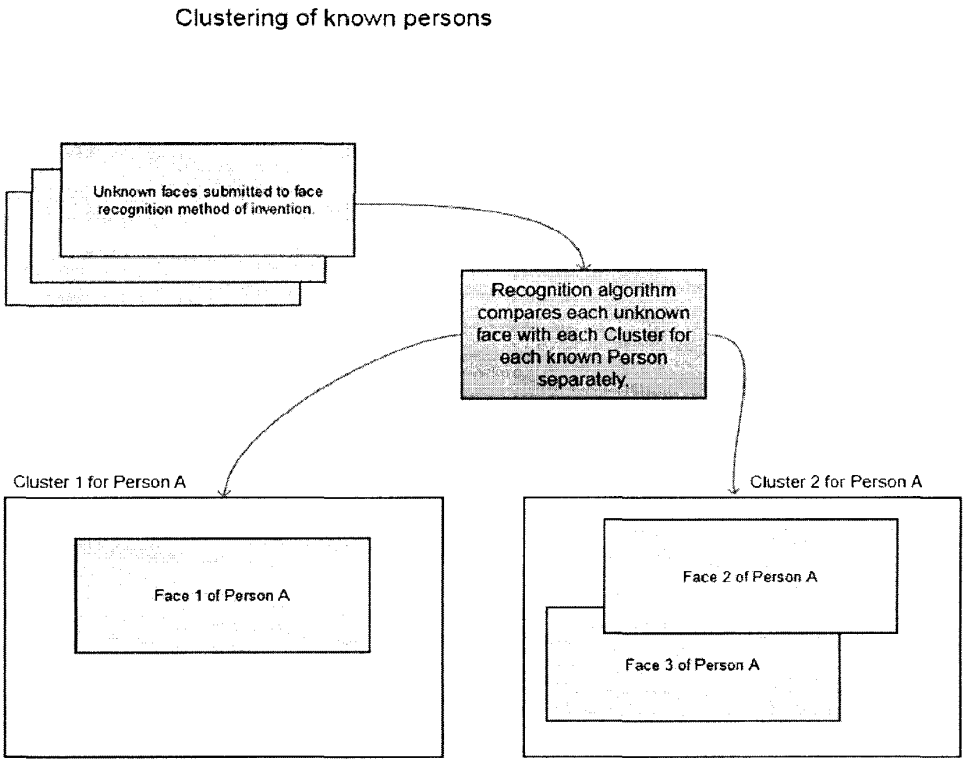

Clustering of known persons
Face 1 of Person A
Recognition algorithm splits clusters of "like" faces based on the face signature distance between each face.
Cluster 1 for Person A
Face 1 of Person A
Cluster 2 for Person A
Face 2 of Person A
Face 3 of Person A

Figure 53


Clustering of known persons
Unknown faces submitted to face recognition method of invention.
Recognition algorithm compares each unknown face with each Cluster for each known Person separately.
Cluster 1 for Person A
Face 1 of Person A
Cluster 2 for Person A
Face 2 of Person A
Face 3 of Person A

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2014/000802

A. CLASSIFICATION OF SUBJECT MATTER
IPC: ***G06K 9/46*** (2006.01), ***G06K 9/62*** (2006.01), ***G06Q 30/02*** (2012.01), ***G06T 3/60*** (2006.01), ***G06T 5/00*** (2006.01)

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC: ***G06K 9/46*** (2006.01), ***G06K 9/62*** (2006.01), ***G06Q 30/02*** (2012.01), ***G06T 3/60*** (2006.01), ***G06T 5/00*** (2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Questel-Orbit, Esp@cenet, Canadian Patent Database, USPTO Database, IEEE Xplore.
Keywords: face, digital, image, detect, recognition, rotation, rotate, horizontal, vertical, plane, suppress, mask.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X, Y	WO2008107002A1 (STEINBERG ET AL.) 12 September 2008 (12-09-2008) -see abstract; -see page 6, line 12 to page 12, line 8; -see figures 2a-5.	1 & 21 2-6, 15-20 and 22-23
Y	US2007098303A1 (GALLAGHER ET AL.) 03 May 2007 (03-05-2007) -see abstract; -see paragraphs [0056]-[0058]; -see figure 1.	2, 3, 15, 17, 18, 22
Y	WO2009082814A1 (GANONG ET AL.) 09 July 2009 (09-07-2009) -see abstract; -see page 4, lines 1-8.	4-6 and 23

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:	
"A" document defining the general state of the art which is not considered to be of particular relevance	
"E" earlier application or patent but published on or after the international filing date	
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention	
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone	
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art	
"&" document member of the same patent family	

Date of the actual completion of the international search 02 January 2015 (02-01-2015)	Date of mailing of the international search report 29 January 2015 (29-01-2015)
Name and mailing address of the ISA/CA Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001-819-953-2476	Authorized officer Hassan Bayaa (819) 997-7810

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US2013057693A1 (BARANEK, JOHN) 07 March 2013 (07-03-2013) -see whole document.	1-24
A	US2013077835A1 (KRITT ET AL.) 28 March 2013 (28-03-2013) -see whole document.	1-24
A	EP1455297A1 (SAMSUNG ELECTRONICS LTD.) 08 September 2004 (08-09-2004) -see whole document.	1-24

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CA2014/000802

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
WO2008107002A1	12 September 2008 (12-09-2008)	WO2008107002A1	12 September 2008 (12-09-2008)
		EP2188759A1	26 May 2010 (26-05-2010)
		JP2010520684A	10 June 2010 (10-06-2010)
		JP4970557B2	11 July 2012 (11-07-2012)
		KR20100015347A	12 February 2010 (12-02-2010)
		KR101247147B1	29 March 2013 (29-03-2013)
		US2010272363A1	28 October 2010 (28-10-2010)
		US8649604B2	11 February 2014 (11-02-2014)
		US2014153780A1	05 June 2014 (05-06-2014)
US2007098303A1	03 May 2007 (03-05-2007)	US2007098303A1	03 May 2007 (03-05-2007)
		CN101300588A	05 November 2008 (05-11-2008)
		EP1955256A1	13 August 2008 (13-08-2008)
		JP2009514107A	02 April 2009 (02-04-2009)
		KR20080060265A	01 July 2008 (01-07-2008)
		WO2007053458A1	10 May 2007 (10-05-2007)
WO2009082814A1	09 July 2009 (09-07-2009)	WO2009082814A1	09 July 2009 (09-07-2009)
		WO2009082814A8	24 February 2011 (24-02-2011)
		CA2711143A1	09 July 2009 (09-07-2009)
		CN102016882A	13 April 2011 (13-04-2011)
		US2010287053A1	11 November 2010 (11-11-2010)
		US8750574B2	10 June 2014 (10-06-2014)
		US2014161326A1	12 June 2014 (12-06-2014)
US2013057693A1	07 March 2013 (07-03-2013)	None	
US2013077835A1	28 March 2013 (28-03-2013)	US2013077835A1	28 March 2013 (28-03-2013)
		US2013077833A1	28 March 2013 (28-03-2013)
EP1455297A1	08 September 2004 (08-09-2004)	EP1455297A1	08 September 2004 (08-09-2004)
		EP1455297B1	28 March 2007 (28-03-2007)
		DE602004005520D1	10 May 2007 (10-05-2007)
		DE602004005520T2	16 August 2007 (16-08-2007)
		KR20040079804A	16 September 2004 (16-09-2004)
		KR100548211B1	02 February 2006 (02-02-2006)
		US2004183951A1	23 September 2004 (23-09-2004)
		US7359529B2	15 April 2008 (15-04-2008)

Electronic Patent Application Fee Transmittal	
Application Number:	14839505
Filing Date:	28-Aug-2015
Title of Invention:	Facial Recognition Authentication System Including Path Parameters
First Named Inventor/Applicant Name:	Kevin Alan Tussy
Filer:	Chad W. Miller/Elizabeth Escoffie
Attorney Docket Number:	FACIAL.0012P

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt	
EFS ID:	30526163
Application Number:	14839505
International Application Number:	
Confirmation Number:	6236
Title of Invention:	Facial Recognition Authentication System Including Path Parameters
First Named Inventor/Applicant Name:	Kevin Alan Tussy
Customer Number:	32856
Filer:	Chad W. Miller
Filer Authorized By:	
Attorney Docket Number:	FACIAL.0012P
Receipt Date:	29-SEP-2017
Filing Date:	28-AUG-2015
Time Stamp:	19:56:10
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$90
RAM confirmation Number	100217INTEFSW00010834502200
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	CWMW12282IDSTRANS.pdf	169392 8da0cfbc7e3f2fc5bafd70086d00bc11d3058f8f	no	1
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	CWMW12280PTO1449.pdf	814721 701fc3d7c86c484a4b3c45c0bf36a30aeb979091	no	9
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Foreign Reference	REF1EP1388802.pdf	750815 082210c933a7c09edb2e4676f7ab8d2f1a937d64	no	18
Warnings:					
Information:					
4	Foreign Reference	REF2EP1455297.pdf	984816 f8930c419eecb70adceed0eac2352e22eecdf00b	no	19
Warnings:					
Information:					
5	Foreign Reference	REF3WO2006130542.pdf	1470800 6bd67801adfaa3c3f142d2002278b0fe0b73e3b4	no	35
Warnings:					
Information:					
6	Foreign Reference	REF4WO2008107002.pdf	1183596 a30508c994ff76b9f97eadb0a8c655d1ecb199d9	no	29
Warnings:					

Information:					
7	Foreign Reference	REF5WO2015070320.pdf	7525397 45fd66d1ff90c6e72103d88ab8223474c7e7b02a	no	124
Warnings:					
Information:					
8	Non Patent Literature	REF1AfterEffectsTutorial173.pdf	867537 139c2aee576ab2e0eeb0fe5b10e47e49318956ff	no	3
Warnings:					
Information:					
9	Non Patent Literature	REF2OpticalIllusionsAnimatedGIF.pdf	501054 434ee9dd06f65be2bee9c29eb62b626abe873d5c	no	3
Warnings:					
Information:					
10	Non Patent Literature	REF3TheUniversalFaceLoginFor5Billion.pdf	574465 cba681bd8d8c2112a23fb4989031208be636d96e	no	3
Warnings:					
Information:					
11	Non Patent Literature	REF4PatchBasedProbabilisticImageQuality.pdf	803052 48355fa9437cb1dd3f9baadcb395d55ad115d0bd	no	8
Warnings:					
Information:					
12	Non Patent Literature	REF5RafalovitchViewfinderFriendsIdeaForFacebook.pdf	144131 dce696578d4f656430d186eb5b7d0c0a8faf5eb1	no	5
Warnings:					
Information:					
13	Non Patent Literature	REF6KishoreHowToAddUploadAndTagYourPictures.pdf	877701 b47b5f70f2de40c9031286480bd523d3af2d866b	no	12
Warnings:					
Information:					

14	Non Patent Literature	REF7BeckerEvaluationofFaceRecognitionTechniques.pdf	78052 1b376ee5c3cd44c10f1ceca9502eb74dc16e94cc	no	2
Warnings:					
Information:					
15	Non Patent Literature	REF8BakerGoogleAndRiyaRecognition.pdf	631186 dc7c806db310a4d5cd17ca875ec6b07dc0f20ce8	no	10
Warnings:					
Information:					
16	Non Patent Literature	REF9PonceRiyaPhotoSharingWithFaceRecognition.pdf	498321 d56e63089b2c52a1940be9d2644d0e50e86ab976	no	3
Warnings:					
Information:					
17	Non Patent Literature	REF10FacebookMakingPhotoTaggingEasier.pdf	180994 e836ccace1cae545baabd362c243b057a85b7f99	no	2
Warnings:					
Information:					
18	Non Patent Literature	REF11MichelsonAutoTagging.pdf	317201 0716c0ffda73fc49eaade96c0ca8eeec9612738a	no	5
Warnings:					
Information:					
19	Non Patent Literature	REF12ArringtonFirstScreenShotsOfRiya.pdf	905717 3dca18d41d3134e27e841f47b735428142472130	no	10
Warnings:					
Information:					
20	Non Patent Literature	REF13ArringtonOjosAutoNameAndTagYourPhotos.pdf	744168 a5fca50a4015948ea0ae168f6a7bd97a7f4810c7	no	9
Warnings:					
Information:					

21	Non Patent Literature	REF14StoneAutotaggingFacebook.pdf	844249 6d95990d3ca9add1db6e61935e7cbf423d110115	no	8
Warnings:					
Information:					
22	Non Patent Literature	REF15SchuonCS229ProjectReport.pdf	284691 034fd7a9d9ffe242b08ef25814ea7fc5ecc1256e	no	5
Warnings:					
Information:					
23	Non Patent Literature	REF16YadavFacebookTheCompleteAutobiography.pdf	2257507 3f250f052214759dd0bc8830c0e350950c90dc31	no	12
Warnings:					
Information:					
24	Non Patent Literature	REF17UnknownWhatDoesItMeanToTag.pdf	264516 a994e1db2447a0fdaa93954b36a8ba4fbb1a5c86	no	2
Warnings:					
Information:					
25	Fee Worksheet (SB06)	fee-info.pdf	30740 5d75aa88afeb3b0196d4e75efa2d78b5141a6e91	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	23704819		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor	:	Kevin Alan Tussy	Group Art Unit: 2436
Appl. No.	:	14/839,505	I hereby certify that this correspondence and all marked attachments are being deposited with the United States Patent Office via EFSWeb filing, on: September 29, 2017 (Date) /Chad W. Miller/ Chad W. Miller Reg. No. 44,943
Filed	:	August 28, 2015	
For	:	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS	
Examiner	:	Shanto Abedin	

THIRD SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Enclosed is form PTO-1449 listing 235 U.S. references, copies of which are not required to be provided in accordance with 37 C.F.R. §1.98(e), 5 foreign references and 17 publications, copies of which are enclosed herewith. This Information Disclosure Statement is being filed after the mailing of the first Office Action on the merits, and therefore the fee of $90.00 in accordance with 37 C.F.R. §1.97(c)(2) and 1.17(p) is submitted herewith.

Respectfully submitted,

Dated: September 29, 2017

By: /Chad W. Miller/
Chad W. Miller
Attorney for Applicant
Registration No. 44,943
Weide & Miller, Ltd.
7251 West Lake Mead Blvd., Suite 530
Las Vegas, NV 89128
(702) 382-4804 (Pacific Time)
cmiller@weidemiller.com

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/839,505	08/28/2015	Kevin Alan Tussy	FACIAL.0012P	6236

32856 7590 09/14/2017

WEIDE & MILLER, LTD.
7251 W. LAKE MEAD BLVD.
SUITE 530
LAS VEGAS, NV 89128

EXAMINER	
ABEDIN, SHANTO	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
09/14/2017	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	14/839,505	TUSSY, KEVIN ALAN	
	Examiner	Art Unit	
	SHANTO M. ABEDIN	2436	

All participants (applicant, applicant's representative, PTO personnel):

(1) *SHANTO M. ABEDIN*. (3)_____.

(2) *CHAD W. MILLER*. (4)_____.

Date of Interview: *13 September 2017*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1*.

Identification of prior art discussed: *US 2014/0123275 A1 (hereinafter Azar et al); US 2014/0165187 A1 (hereinafter Daesung et al)*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant's representative gave a summary of the claimed invention and discussed how it differed from the cited references (especially in terms of using a movement detection sensor for detecting movement of the mobile/ imaging device) Examiner acknowledged some of the differences between the claimed invention and the cited arts. However, applicant's representative was suggested that further incorporation from the specification or dependent claims might be needed in order to make the claimed invention distinguishable over the cited prior arts.
Copy of the interview agenda is enclosed herein.

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☒ Attachment

/SHANTO M ABEDIN/ Primary Examiner, Art Unit 2436	

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

———

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Topics For Discussion During Telephone Interview

(Informal - Not For Entry)

1. Discuss Possible Claim Amendments to Make Clear that Mobile Device (phone) is item moving and Non-Camera Sensors from Phone provide Movement Information – not the user's head or face expression. See paragraph [0038] of the Daesung reference.

2. Discuss Benefits of Moving Mobile Device Instead of Head
    a. Easy to Spoof Head Movement or Facial Expression – Software can take 2-D photo from Facebook or LinkedIn and turn it into movable 2-D or moveable 3-D video / image
        i. See Crazy Talk 8 software at following links:

https://www.reallusion.com/crazytalk/features.html
https://www.youtube.com/watch?v=3iGxo4rHzM4

    b. By Using Mobile Device Movement Sensors (accelerometer, gyroscope, . . .) it provides confirmation that mobile device is moving, and thus there is a live person moving the device at the same speed/acceleration/path as used when enrolled.

    c. Technically, it is very difficult to spoof mobile device sensor data. It would require hacking into the phone. And, even if hacked, the 'created movement data' would have to have to generally match the enrollment data (match speed and acceleration of mobile device). This is much harder to spoof that just an image or screen display of a person rotating their head or winking, which could be computer generated.

d. Movement data is generated during capturing of second image – claim 1 – very difficult to spoof since concurrent with second image capture, the movement data is also captured. This allows syncing image with movement. This is very difficult to fake. For example, because the second image is captured during movement this further prevents fraud.

e. In addition, the mobile device motion sensors will detect movement from first position to second position and thus expect that the second image must also correspond to an image captured at an expected second mobile device position. If the second image is not captured from the expected second mobile device position, then fraud is likely.

f. Image capture from different mobile device positions also prevents fraud due to detectible changes in three dimensionality of a human face at different positions. The camera will capture a different perspective of a three dimensional facial features (nose, ears, eyes) at different mobile device positions that are not captured if only the head is moved to the side or a person winks. Movement could be from far away (arm's length) and the close to face (arm bent) or arc across and around front of face from side to side. At different image capture locations, the three dimensionality of the face is captured, which is not part of simply having the person wink or move head to the side as proposed in the prior art.

g. Having movement of the mobile device, instead of just movement of the user's head, provides additional information about the background of the user. Movement of the mobile device changes not only the perspective view of the user's face, but also the background. If only the head moves to the side or the user blinks, the background does not really change. Thus, claimed system is much harder to spoof, thereby doing a better job at preventing fraud.

UNITED STATES PATENT AND TRADEMARK OFFICE

USPTO Automated Interview Request (AIR)

Sep 6 2017

This paper requesting to schedule and/or conduct an interview is appropriate because:

This submission is requested to be accepted as an authorization for this interview to communicate via the internet. Recognizing that Internet communications are not secure, I hereby authorize the USPTO to communicate with the undersigned concerning scheduling of the interview via video conference, instant messaging, or electronic mail, and to conduct the interview in accordance with office practice including video conferencing.

Name(s):
Chad W. Miller

S-signature:
/Chad W Miller/

Registration Number:
44943

U.S. Application Number:
14839505

Confirmation Number:
6236

E-mail Address:
cmiller@weidemiller.com

Phone Number:
7023824804

Proposed Time of Interview:
9-14-2017 1:30 PM ET

Prefered Interview Type:
Telephonic

I am the applicant or applicant's representative for this application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/839,505	08/28/2015	Kevin Alan Tussy	FACIAL.0012P	6236

32856 7590 07/17/2017

WEIDE & MILLER, LTD.
7251 W. LAKE MEAD BLVD.
SUITE 530
LAS VEGAS, NV 89128

EXAMINER	
ABEDIN, SHANTO	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
07/17/2017	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 14/839,505	Applicant(s) TUSSY, KEVIN ALAN	
	Examiner SHANTO M. ABEDIN	Art Unit 2436	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08/28/2015*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-21* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-7 and 9-21* is/are rejected.

8)☒ Claim(s) *8* is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *08/28/2015* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *01/13/2016; 02/22/2016; and 03/02/2017*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

DETAILED ACTION

1. This office action is in response to the communication filed on 08/28/2015. Claims 1-21 are pending in the application. Claim 8 is objected. Claims 1-7 and 9-21 have been rejected.

Information Disclosure Statement

2. The information disclosure statements (IDS) submitted on 01/13/2016, 02/22/2016 and 03/02/2017 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statements are being considered by the examiner.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103 are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. Claims 1-3, 7, 11-18 and 20 are rejected under 35 U.S.C. 103 as being unpatentable over US 2014/0123275 A1 (hereinafter Azar et al) in view of US 2014/0165187 A1 (hereinafter Daesung et al)

Regarding claim 1, Azar et al teaches a method for enrolling and authenticating a user in an authentication system via a user's a mobile computing device comprising a camera and at least one movement detecting sensor, the method comprising:

capturing enrollment biometric information from at least one first image of the user, the first image recorded by the camera of the mobile device (Note Para 027, 032: storing user image in database);

storing the enrollment biometric information on a memory (Note Para 027, 032);

capturing authentication biometric information from at least one second image of the user, the second image recorded by the camera of the mobile device (Note Para 027, 034: receiving new/ updated image of the user for authentication);

comparing the authentication biometric information to the stored enrollment biometric information to determine whether the authentication biometric information meets a predetermine similarity threshold as compared to the enrollment biometric information (Note Para 005: matching biometric information to a threshold value; Para 027, 032, 034, 037: authenticating using facial biometrics when meets threshold value; matching with the database image) ;

when the authentication biometric information sufficiently corresponds with the enrollment biometric information (Note Para 027, 032, 034)

Azar et al fails to teach expressly recording, during imaging of the at least one second image, path parameter data from the at least one movement detecting sensor, the path parameter data representing an authentication movement of the mobile device; and comparing the authentication movement of the mobile device to an expected movement of the mobile device to determine whether

the authentication movement meets a predetermine similarity threshold as compared to the expected movement; and when the authentication movement a predetermine similarity threshold as compared to with the expected movement, authenticating the user.

However, Daesung et al teaches recording, during imaging of the at least one second image, path parameter data from the at least one movement detecting sensor, the path parameter data representing an authentication movement of the mobile device (Note Figure 3: steps 200 and 210; Para 012-014: registered movement pattern; Para 040: rotation direction of head); and comparing the authentication movement of the mobile device to an expected movement of the mobile device to determine whether the authentication movement meets a predetermine similarity threshold as compared to the expected movement (Note Para 017, 038-040, 048, 051: matching movement pattern; authenticating modified face movement of user); and when the authentication movement a predetermine similarity threshold as compared to with the expected movement, authenticating the user (Note Para 017, 039, 048, 051)

Daesung et al and Azar et al are analogous art because they are from the same field of endeavor of authenticating users using biometric/ facial information. Therefore, at the time of invention, it would have been obvious to a person of ordinary skill in art to modify Azar et al method/ system to further include the features of when the authentication movement a predetermine similarity threshold as compared to with the expected movement, authenticating the user in order to provide users with a dynamic and enhanced authentication mechanism utilizing facial movement information (Note Daesung et al, Para 006-007, 016-017)

Regarding claim 2, Daesung et al teaches the method according to claim 1, further comprising capturing, during imaging of the at least one first image, enrollment path parameters via

the at least one movement detecting sensor (Note Para 013-014: registered movement pattern), the enrollment path parameters indicating an enrollment movement of the mobile device, and defining the expected movement as the enrollment movement (Note Para 038-040)

Regarding claim 3, Daesung et al teaches the method according to claim 1, wherein the at least one first image and the at least one second image of the user include an image of the user's face, and the enrollment biometric information and the authentication biometric information comprise facial recognition information (Note Para 027, 039, 048, 051: authentication using registering and using face/ biometric recognition)

Regarding claim 7, Azar et al teaches a facial authentication system utilizing a user's mobile device, the mobile device comprising a camera (Note Figure 1.105: camera) and at least one movement detecting sensor (Note Figure 1.113: feature tracking), the authentication system comprising:

an authentication server comprising a processor, a memory (Note Figure 1.101: device; 1.109: microprocessor), and at least one transceiver configured to transmit data from the authentication server and received data;

one or more memories configured to store one or more databases (Note Figure 1.107: database), the one or more databases configured to store authentication information profiles; and

machine readable instructions that are stored on the memory of the authentication server (Note Figure 1.101: device) which when executed by the processor, cause the authentication server to:

receive enrollment biometrics from the mobile device, the enrollment biometrics comprising facial recognition data processed from at least one first image of the user's face obtained via the camera of the mobile device (Note Para 027, 032: storing user image in database);

store the enrollment biometrics in the one or more databases (Note Para 027, 032: storing user image in database) and associate the enrollment biometric data with the user authentication information profile (Note Para 034-035: stored password/ login information);

receive authentication biometrics from the mobile device during an authentication attempt by the user, the authentication biometrics comprising facial recognition data processed from at least one second image of the user's face, the image obtained from the camera of the mobile device (Note Para 027, 034: receiving new/ updated image of the user for authentication);

authenticate or not authenticate the user based on a comparison match rate of the authentication biometrics (Note Para 027, 032, 034)

Azar et al fails to teach expressly receive authentication movement information from the mobile device, the authentication movement information comprising data regarding movement of the mobile device during imaging of the at least one second image as detected by the at least one movement detecting sensor in the mobile device; and compare the authentication biometrics and the authentication movement information with the enrollment biometrics and expected movement information stored in the database with the user authentication information profile; and authenticate or not authenticate the user based on the authentication movement with the enrollment biometrics and the expected movement.

However, Daesung et al teaches receive authentication movement information from the mobile device, the authentication movement information comprising data regarding movement of

the mobile device during imaging of the at least one second image as detected by the at least one movement detecting sensor in the mobile device (Note Para 017, 038-040, 048, 051: matching movement pattern; authenticating modified face movement of user); and compare the authentication biometrics and the authentication movement information with the enrollment biometrics and expected movement information stored in the database with the user authentication information profile (Note Para 017, 040, 048, 051); and authenticate or not authenticate the user based on the authentication movement with the enrollment biometrics and the expected movement (Note Para 017, 039, 048, 051)

Daesung et al and Azar et al are analogous art because they are from the same field of endeavor of authenticating users using biometric/ facial information. Therefore, at the time of invention, it would have been obvious to a person of ordinary skill in art to modify Azar et al method/ system to further include the features of authenticate or not authenticate the user based on the authentication movement with the enrollment biometrics and the expected movement in order to provide users with a dynamic and enhanced authentication mechanism utilizing facial movement information (Note Daesung et al, Para 006-007, 016-017)

Regarding claim 11, Azar et al teaches the facial authentication system of claim 7, wherein the authentication server or mobile device estimates at least one of a gender, age, and ethnicity of a face imaged in the at least one first image (Note Para 034: authenticating using facial, ageing, color of skin information), the authentication server estimates at least one of a gender, age, and ethnicity of the face imaged in the at least one second image (Note Para 034-035), and the authentication server authenticates or does not authenticate the user based on a comparison match rate of at least

one of a gender, age, and ethnicity detected in the at least one first image and the at least one second image in relation to a comparison match rate threshold (Note Para 034-035)

Regarding claim 12, Azar et al teaches the facial authentication system of claim 7, wherein the comparison match rate threshold required for authentication is variable (Note Para 005, 037)

Regarding claim 13, Azar et al teaches the facial authentication system of claim 12, wherein the comparison match 10 rate threshold increases based on a number of successful authentications (Note Para 027)

Regarding claim 14, Azar et al teaches the facial authentication system of claim 12, wherein the comparison match rate threshold increases over time (Note Para 027, 037)

Regarding claim 15, Azar et al teaches a method for authenticating a user in an authentication system via a user's camera equipped computing device, the method comprising:

capturing at least one first image of the user taken with the camera of the computing device at a first distance from the user (Note Para 027, 032);

processing the at least one first image to obtain first biometric data based on facial recognition data from the at least one first image (Note Para 027, 032);

processing the at least one second image to obtain second biometric data based on facial recognition data from the at least on second image (Note Para 027, 034);

comparing the first biometric data to the second biometric data (Note Para 027, 032, 034);

when the first biometric data does not match the second biometric data within a predetermined threshold, authenticating the user (Note Para 027, 032, 034); and

when the first biometric data matches the second biometric data within a predetermined threshold, denying access to the user (Note Para 027, 032, 034)

Azar et al fails to teach expressly capture at least one second image of the user taken with the camera of the computing device at a second distance from the user, the second distance being different from the first distance.

However, Daesung et al teaches capture at least one second image of the user taken with the camera of the computing device at a second distance from the user, the second distance being different from the first distance (Note Figure 3: steps 200 and 210; Para 012-014: registered movement pattern; Para 038-040, 048: matching rotational direction, movement pattern)

Daesung et al and Azar et al are analogous art because they are from the same field of endeavor of authenticating users using biometric/ facial information. Therefore, at the time of invention, it would have been obvious to a person of ordinary skill in art to modify Azar et al method/ system to further include the features of capture at least one second image of the user taken with the camera of the computing device at a second distance from the user, the second distance being different from the first distance in order to provide users with a dynamic and enhanced authentication mechanism utilizing movement/ distance information associated with the image (Note Daesung et al, Para 006-007, 016-017)

Regarding claim 16, Azar et al teaches the method according to claim 15, further comprising:

capturing at least one first enrollment image of the user taken with the camera of the computing device at the first distance from the user (Note Para 027, 032, 034);

processing the at least one first enrollment image to obtain first enrollment biometric data based on facial recognition data from the at least one first enrollment image (Note Para 027, 032, 034);

comparing the first biometric data to the first enrollment biometric data (Note Para 027, 032, 034); and

authenticating the user when the first biometric data matches the first enrollment biometric data within a predetermined threshold (Para 027, 032, 034, 037: authenticating using facial biometrics when meets threshold value)

Regarding claim 17, Daesung et al teaches the method according to claim 16, further comprising: capturing at least one second enrollment image of the user taken with the camera of the computing device at the second distance from the user (Para 014, 040, 048);

processing the at least one second enrollment image to obtain second enrollment biometric data based on facial recognition data from the at least one second enrollment image (Para 014, 038-040, 048);

comparing the second biometric data to the second enrollment biometric data; and authenticating the user when the second biometric data matches the second enrollment biometric data within a predetermined threshold (Para 014, 038-040, 048)

Regarding claim 18, Azar et al teaches method according to claim 15, wherein the mobile device provides real time video feedback on a display of the mobile device during imaging (Note Para 039, 042)

Regarding claim 20, Azar et al teaches the method according to claim 15, further comprising displaying a pattern on the display of the mobile device during the imaging (Note Para 027, 032,

034); and processing the at least one first image or the at least one second image to detect a reflection of the pattern off of an eye or face of the user (Note Para 027, 032, 034)

4. Claims 4-6, 9-10 and 21 are rejected under 35 U.S.C. 103 as being unpatentable over Azar et al in view of Daesung et al further in view of US 9,607,138 B1 (hereinafter Baldwin et al)

Regarding claim 4, Modified Daesung et al-Azar et al method fails to teach expressly the method according to claim 1, further comprising: capturing enrollment device information during imaging of the at least one first image; storing the enrollment device information on the memory; capturing authentication device information during imaging of the at least on second image; and comparing the authentication device information with the enrollment device information to determine whether the authentication device information sufficiently corresponds to the enrollment device information.

However, Baldwin et al teaches capturing enrollment device information during imaging of the at least one first image (Note Column 17, lines 30-58); storing the enrollment device information on the memory; capturing authentication device information during imaging of the at least on second image (Note Column 17, lines 30-58); and comparing the authentication device information with the enrollment device information to determine whether the authentication device information sufficiently corresponds to the enrollment device information (Note Column 2, starts a line 16; Column 17, lines 30-58)

Baldwin et al and Azar et al are analogous art because they are from the same field of endeavor of authenticating users using biometric/ facial information. Therefore, at the time of invention, it would have been obvious to a person of ordinary skill in art to modify Azar et al

method/ system to further include the features of comparing the authentication device information with the enrollment device information to determine whether the authentication device information sufficiently corresponds to the enrollment device information in order to provide users with an enhanced authentication mechanism utilizing both device information and facial movement or liveness information (Note Baldwin et al, Note Column 2, starts a line 10)

Regarding claim 5, Baldwin et al teaches the method according to claim 4, wherein the device information comprises at least one of the following: a device manufacturer, model number, serial number, and mobile network information (Note Column 17, lines 30-58)

Regarding claim 6, Baldwin et al teaches the method according to claim 1, wherein at least one movement detecting sensor comprises at least one of the following: an accelerometer, a magnetometer, and a gyroscope (Note Column 17, starts at line 31)

Regarding claim 9, Baldwin et al teaches the facial authentication system of claim 7, wherein the authentication server detects the presence or absence of banding in the at least one second image (Note Column 5, starts at line 30: face/ edge detection algorithm)

Regarding claim 10, Baldwin et al teaches the facial authentication system of claim 7, wherein the authentication server detect the present or absence of a screen edge in the at least one second image (Note Column 5, starts at line 30; Column 9, starts at line 15)

Regarding claim 21, Baldwin et al teaches the method according to claim 20, wherein the pattern is a unique one-5 dimensional or two-dimensional barcode (Note Column 17, lines 30-58)

5. Claim 19 is rejected under 35 U.S.C. 103 as being unpatentable over Azar et al in view of Daesung et al further in view of US 2014/0169643 A1 (hereinafter Todoroki)

Regarding claim 19, Azar et al teaches the method according to claim 15, further comprising processing the at least one first image and the at least one second image (Note Para 039-042)

Modified Daesung et al- Azar et al method fails to disclose expressly distorting the at least one first image and the at least one second image prior to processing.

However, Todoroki teaches distorting the at least one first image and the at least one second image prior to processing (Note Para 064, 089)

Todoroki and Azar et al are analogous art because they are from the same field of endeavor of authenticating users using biometric/ facial information. Therefore, at the time of invention, it would have been obvious to a person of ordinary skill in art to modify Azar et al method/ system to further include the features of distorting the at least one first image and the at least one second image prior to processing in order to provide users with an improved authentication/ movement detection mechanism that would further utilize image distortion information (Note Todoroki, Para 018-019, 089)

Allowable Subject Matter

6. Claim 8 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

7. A shortened statutory period for response to this action is set to expire in 3 (Three) months and 0 (Zero) days from the mailing date of this letter. Failure to respond within the period for response will result in ABANDOMENT of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M. Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 8:30 AM to 6:30 PM. Examiner interviews are available via

telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Shewaye Gelagay, can be reached on 571-272-4219. The RightFax number for faxing directly to the examiner is 571-273-3551.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/SHANTO M ABEDIN/

Primary Examiner, Art Unit 2436

Notice of References Cited	Application/Control No. 14/839,505	Applicant(s)/Patent Under Reexamination TUSSY, KEVIN ALAN	
	Examiner SHANTO M. ABEDIN	Art Unit 2436	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-9,607,138 B1	03-2017	Baldwin; Leo Benedict	G06F21/32	1/1
*	B	US-8,856,541 B1	10-2014	Chaudhury; Krishnendu	G06F21/32	382/115
*	C	US-2014/0198959 A1	07-2014	DERAKHSHANI; Reza	G06K9/00597	382/117
*	D	US-2014/0165187 A1	06-2014	Daesung; Kim	G06K9/00335	726/19
*	E	US-2014/0059673 A1	02-2014	Azar; Cyrus	G06F21/32	726/19
*	F	US-2014/0123275 A1	05-2014	Azar; Cyrus	H04W12/06	726/19
*	G	US-2014/0337948 A1	11-2014	Hoyos; Hector	H04L63/0861	726/7
*	H	US-2014/0169643 A1	06-2014	Todoroki; Yasuhiro	G06K9/00288	382/118
*	I	US-2015/0378433 A1	12-2015	Savastinuk; Paul Aksenti	G06K9/00255	345/156
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Hagai Aronowitz et al, Multi-Modal Biometrics for Mobile Authentication, IJCB, 2014
	V	Silvio Barra et al, FAME: Face Authentication for Mobile Encounter, IEEE, 2013
	W	Girija Chetty et al, Liveness Verification in Audio-Video Speaker Authentication, Australian Speech Science & Technology Association Inc., 2004
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	109346	(face or facial)(authenticat$4 or verification or identity)(image or picture)	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:30
L2	55465	L1(face or facial or authenticat$4 or verification or identity)same(image or picture)	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:31
L3	50886	L1(face or facial)same(authenticat$4 or verification or identity or image or picture)	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:31
L4	60823	L2 OR L3	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:31
L5	46304	L4 (movement or position or angle or chang$4)same(camera or device or face or facial)	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:32
L6	30508	L4 (movement or position or angle or chang$4 or different)same(camera or face or facial)same(image or picture or second)	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:33
L7	48428	L5 OR L6	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:34
L8	9132	L7 (threshold)(recognition)(authenticat$4)	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:34
L9	7300	L7 (threshold or within or expect$4)near5(distance or position$4 or movement or direction or angle)same(chang$4 or second or camera or device)same(picture or image or face or facial)	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:36
L10	2378	L7 (threshold or within or expect$4 or meet$4 or met)near5(distance or position$4 or movement or direction or angle or chang$4)same(picture or image or face or facial or second).clm.	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:37
L11	3001	L7 (threshold or within or expect$4 or meet$4 or met or authenticat$4)near7(distance or position$4 or movement or direction or angle or chang$4)same(picture or image or face or facial or second).clm.	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:38
L12	15656	L8 or L9 or L11	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:38
L13	1	14/839505	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:38
L14	1	L13 (path)	US-	AND	OFF	2017/06/28

			PGPUB; USPAT			19:39
L15	6810	L12 (path or direction or chang$4 or motion)same(parameter or angle or trajectory or different)(enrollment or register$4)(recognition)	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:41
L16	793	L12 (path or direction or chang$4 or motion or movement or mov$4)same(parameter or angle or trajectory or different or camera or device or imaging)same(enrollment or register$4 or recognition or face).clm.	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:43
L17	1811	L15 (authenticat$4 or fac$4 or biometric or chang$4 or movement).ab.	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:44
L18	5494	L12 (path or direction or chang$4 or motion)same(parameter or angle or trajectory or different)same(device or camera or image or picture)(enrollment or register$4)(recognition)	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:45
L19	1218	L12 (path or direction or chang$4 or motion)same(parameter or angle or trajectory or different)same(device or camera or image or picture)(enrollment or register$4)(recognition)(authenticat$4 or login or identity).clm.	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:45
L20	2968	L16 or L17 or L19	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:45
L21	10058	(G06F21/34 OR G06F21/32).cpc.	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:46
L39	23021	(G06F21/34 OR G06F21/32 OR G06F21/6218 OR H04L63/0861).cpc.	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:00
L40	516	L20 L39	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:00
L41	7334	(726/6-7).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/28 20:00
L42	11509	(713/168,182).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/28 20:00
L43	17922	L41 OR L42	US-PGPUB; USPAT	OR	OFF	2017/06/28 20:01
L44	9107	(455/410,411).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/28 20:01
L45	26554	L41 OR L42 OR L44	US-PGPUB; USPAT	OR	OFF	2017/06/28 20:01
L46	93	L20 L45	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:01

L47	561	L40 OR L46	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:01
L48	447	L47 (movement or position or angle or chang$4 or different or moving)same(camera or device)same(image or picture or face)	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:03
L49	247	L47 (movement or position or angle or chang$4 or different or moving)near5(camera or device)same(image or picture or face)	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:03
L50	323	L47 (path or direction or chang$4 or motion)same(parameter or angle or trajectory or different)same(device or camera or image or picture)(enrollment or register$4)(recognition)(authenticat$4 or login or identity).clm.	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:04
L51	292	L39 L50	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:04
L52	149	L49 L51	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:04
L53	390	L49 OR L51	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:04
L54	71	L53 (authenticat$4 or identity or login or verification).ab.(movement or path or direction or moving or chang$4 or angle or recognition or enrolled or registered).ab. (camera or image or picture or face or facial or video).ab.	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:06
L55	49	L52 L54	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:06
L56	171	L52 OR L54	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:06
L57	99	L56(movement or angle or distance or moving or motion or trajectory)near7(camera or device or position or distance)same(image or picture or face)same(chang$4 or different or second)	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:08
L58	48	L57(authenticat$4 or identity or login or verification).ab.(movement or path or direction or moving or chang$4 or angle or recognition or enrolled or registered).ab. (camera or image or picture or face or facial or video).ab.	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:08
L59	58	L55 OR L58	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:09
L60	31	L59 @ad<"20140828"	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:09
L61	12	L60(movement or angle or distance or moving or motion or trajectory or path)near7(camera or device or moving or	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:14

		position or distance)near5(chang$4 or different or second or predetermined or enroll$4)				
L62	71	L56(authenticat$4 or identity or login or verification).ab.(movement or path or direction or moving or chang$4 or angle or recognition or enrolled or registered).ab. (camera or image or picture or face or facial or video).ab.	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:17
L63	122	L57 OR L62	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:17
L64	89	L63 (line or path)	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:17
L65	70	L63 (line or path)same(moving or camera or device)	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:18
L66	51	L63 (line or path)near7(moving or camera or device)	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:18
L67	27	L66 @ad<"20140828"	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:18
L68	52	L60 OR L67	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:22
L69	17	L68 (login)	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:22
L70	214	L53(movement or angle or distance or moving or motion or trajectory or path or position or distance)near7(camera or device or terminal or imaging)near5(chang$4 or different or second or predetermined or enroll$4 or face)	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:24
L71	2555	L39 L45	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:25
L72	19	L70 L71	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:25
L73	9	L72 @ad<"20140828"	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:25
L74	47020	L39 OR L45	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:26
L75	214	L70 L74	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:27
L76	238	L57 OR L62 OR L75	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:27
L77	43	L76(movement or angle or distance or moving or motion or trajectory or path or position or distance)near7(camera or device or terminal or imaging)near5(chang$4 or	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:28

		different or second or predetermined or enroll$4 or face or threshold or meet$4).clm.				
L78	25	L77 @ad<"20140828"	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:28
L79	21	L78(line or path or direction)(login or authenticat$4)	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:28
L80	24	L78(line or path or direction or recognition) (login or authenticat$4)	US-PGPUB; USPAT	AND	OFF	2017/06/28 20:28

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L24	88	face.ti. (authenticat$4).ab.	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:49
L25	53	facial.ab. (authenticat$4).ab. (chang$4 or movement).clm.	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:50
L26	6	L24 L25	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:50
L27	135	L24 OR L25	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:50
L28	26	L27 ((authenticat$4 or identity)(angle or direction or movement)(change or second)).clm.	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:50
L29	31	L26 OR L28	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:51
L30	85648	(path or direction or chang$4 or motion or movement or mov$4)same(parameter or angle or trajectory or different or camera or device or imaging)same(enrollment or register$4 or recognition or face).clm.	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:51
L32	266	L30 (path or direction or chang$4 or motion)same(parameter or angle or trajectory or different)same(device or camera or image or picture)(enrollment or register$4) (recognition)(authenticat$4 or login or identity).clm.	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:52
L33	40426	L30 (authenticat$4 or fac$4 or biometric or chang$4 or movement).ab.	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:52
L34	3630	L33 (threshold or within or expect$4 or meet$4 or met or authenticat$4)near7(distance or position$4 or movement or direction or angle or chang$4)same(picture or image or face or facial or second).clm.	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:52
L35	2435	L34 (movement or position or angle or chang$4 or different)same(camera or face or facial)same(image or picture or second)	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:53

L36	2673	L32 OR L35	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:53
L37	287	L36 (device or camera or moving)near5(direction or path or trajectory or movement)same(register$4 or enroll$4 or compar$4 or meet$4 or threshold)	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:54
L38	4	L29 L37	US-PGPUB; USPAT	AND	OFF	2017/06/28 19:55

6/ 28/ 2017 8:33:59 PM

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

SHEET 1 OF 1

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2431

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2012/0140993	06/12	Bruso, et al.			
		2014/0123275	05/14	Azar, et al.			

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO
		KR 20130097581	09/13	KR (abstract, description & claims translation only)			X	
		CN 103593594 2013	02/14	CN (abstract, description & claims translation only)			X	

EXAMINER INITIAL		**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)
		Girija Chetty and Michael Wagner, "Automated lip feature extraction for liveness verification in audio-video authentication", Human Computer Communication laboratory School of Information Sciences and Engineering, University of Canberra, Australia, Proc. Image and Vision Computer (2004), 1 January, 2004, 6 pages.

EXAMINER	/SHANTO ABEDIN/	DATE CONSIDERED	06/29/2017

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

CWM-W-10610

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	50	"20030095053" "20060224523" "20140022179" "20140173443" "20140337791" "20140351761" "20150074615" "20150148106" "20150227286" "20160026425" "20120140993" "20140123275" "20100310133" "5956122".pn. "7428320".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/06/29 19:15
L2	6	L1 (movement or moving or path or line)same(camera or device or mobile or picture or image)same(face or angle or distance or proximity or predetermined or expected)same(met or meet$4 or threshold or within or second)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2017/06/29 19:18
L3	3	L1 (movement or moving or path or line)same(camera or device or mobile or picture or image)same(face or angle or distance or proximity or predetermined or expected)same(met or meet$4 or threshold or within or second) (enrollment)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2017/06/29 19:19
L4	210	(authenticat$4).ab. (movement or moving or path or line)same(camera or device or mobile or picture or image)same(face or angle or distance or proximity or predetermined or expected)same(met or meet$4 or threshold or within or second) (enrollment)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2017/06/29 19:20
L5	145	L4 (face or biometric)(picture or image)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2017/06/29 19:20
L6	31243	(G06F21/34 OR G06F21/32).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2017/06/29 19:20
L7	64	L5 L6	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2017/06/29 19:21

L8	54	L7 (face)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2017/06/29 19:21
L9	54	L7 (face or facial)(recognition or enrollment)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2017/06/29 19:22
L10	35	L9 (device or camera)same(identifier or number)same(model or network or manufacturer)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2017/06/29 19:23
L11	36	L9 (device or camera)same(identifier or number or "ID")same(model or network or manufacturer)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2017/06/29 19:23
L12	24	L11 @ad<"20140828"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2017/06/29 19:23
L13	26359	(726/2-7).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/29 19:24
L14	6	L12 L13	US-PGPUB; USPAT	AND	OFF	2017/06/29 19:24
L15	24	L12(authenticat$4).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2017/06/29 19:24
L16	18	L12(authenticat$4).ab. (movement or moving or path or line)same(camera or device or mobile or picture or image)same(face or angle or distance or proximity or predetermined or expected)same(met or meet$4 or threshold or within or second) (enrollment)(recognition)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2017/06/29 19:25
L17	18	L14 OR L16	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	AND	OFF	2017/06/29 19:25

			IBM_TDB			
L18	16	L17 (threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2017/06/29 19:25
L19	41	"9607138".pn. "20060288234" "20140337948" "20140165187" "20140059673" "20140123275" "20140310803" "20140197922" "20150031333" "20150378433"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/06/29 19:32
L20	10	L19(device or camera)same(identifier or number or "ID")same(model or network or manufacturer)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2017/06/29 19:33
L21	8	L19(enrollment)(recognition)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2017/06/29 19:33
L22	12	L20 OR L21	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2017/06/29 19:33
L23	6	L22 (path or line)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2017/06/29 19:33
L24	35	L19 NOT L23	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2017/06/29 19:35
L25	7	L24 (path or line or movement or moving or direction)near3(camera or device)same(threshold or predetermined or meet$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2017/06/29 19:36
L27	6	L24 (path or line or movement or moving or direction)near3(camera or device)same(threshold or predetermined or meet$4)(image or picture)same(face	US-PGPUB; USPAT; USOCR; FPRS; EPO;	AND	OFF	2017/06/29 19:37

		or enrolled or camera)	JPO; DERWENT; IBM_TDB				

6/29/2017 7:40:43 PM
C:\Users\sabedin\Documents\EAST\Workspaces\14570611.wsp

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

SHEET 1 OF 1

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2431

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		5,956,122	09/99	Doster			
		7,428,320	09/08	Northcott, et al.			
		2010/0310133	12/10	Mason, et al.			
		8,280,120	10/12	Hoyos, et al.			
		8,411, 909	04/13	Zhao, et al.			

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
							YES	NO

EXAMINER INITIAL		**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 06/29/2017

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

CWM-W-10485

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14839505	TUSSY, KEVIN ALAN
	Examiner	Art Unit
	SHANTO M ABEDIN	2436

CPC- SEARCHED		
Symbol	Date	Examiner
CPC search: (G06F21/34 OR G06F21/32 OR G06F21/6218OR H04L63/0861).cpc.	06/28/2017	SA

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	6-7	06/28/2017	SA
713	168, 182	06/28/2017	SA
455	410, 411	06/28/2017	SA

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor Assignee/ Double Patenting search	06/28/2017	SA
CPC and USPC classification search (with limited texts)	06/28/2017	SA
EAST databases text search (see search history)	06/28/2017	SA
EAST databases text search (see search history)	06/29/2017	SA
NPL: Google Scholar, IEEE Explore databases search (see search history)	07/09/2017	SA

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
Claim Interference Search	See EAST Search History	06/29/2017	SA

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	11	"9607138".pn. "20140337948" "20140197922" "20140165187" "20140059673" "20140123275" "20150378433"	US-PGPUB; USPAT	OR	ON	2017/07/06 21:10
L2	7	L1 (area)same(screen)	US-PGPUB; USPAT	AND	ON	2017/07/06 21:12
L3	4	L1 (area)same(screen)same(face or plac$4 or prompt$4)	US-PGPUB; USPAT	AND	ON	2017/07/06 21:13
L4	1	L1 (area or size)same(screen or display$4)same(face or path or movement or moving)same(plac$4 or prompt$4)	US-PGPUB; USPAT	AND	ON	2017/07/06 21:14
L5	1	L4 (area or size)same(screen or display$4 or prompt$4)same(face or path or movement or moving or plac$4)	US-PGPUB; USPAT	AND	ON	2017/07/06 21:15
L6	1	L4 OR L5	US-PGPUB; USPAT	AND	ON	2017/07/06 21:15

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L7	9466	(authenticat$4)(face)(camera)(area or size)same(screen or display$4 or prompt$4)same(face or path or movement or moving or plac$4)	US-PGPUB; USPAT	AND	ON	2017/07/06 21:16
L8	725	(authenticat$4).clm.(image or picture).clm.(face)(camera)(area or size)same(screen or display$4 or prompt$4)same(face or path or movement or moving or plac$4 or mov$3)	US-PGPUB; USPAT	AND	ON	2017/07/06 21:17
L9	628	L7(area or size)same(screen or display$4 or prompt$4 or different)same(face or path or movement or moving or plac$4 or mov$3 or distance).clm.	US-PGPUB; USPAT	AND	ON	2017/07/06 21:18
L10	1276	L8 OR L9	US-PGPUB; USPAT	AND	ON	2017/07/06 21:18
L11	571	L10(camera)same(smart$device or smart$phone or mobile)	US-PGPUB; USPAT	AND	ON	2017/07/06 21:19
L12	450	L11(authenticat$4 or authorized or registration or registered)same(data or profile or stored or information or account or identifier)same(user or device)(face or facial)(moving or movement)(direction or path or line)	US-PGPUB; USPAT	AND	ON	2017/07/06 21:20
L13	224	L12(area or size)same(screen or display$4 or	US-	AND	ON	2017/07/06

		prompt$4 or different)same(face or image or picture)same(path or movement or moving or plac$4 or mov$3 or distance)same(user or camera or device)	PGPUB; USPAT			21:21
L14	47	L13(authenticat$4).ab.(image or picture).clm. (face)	US-PGPUB; USPAT	AND	ON	2017/07/06 21:22
L15	11	"9607138".pn. "20140337948" "20140197922" "20140165187" "20140059673" "20140123275" "20150378433"	US-PGPUB; USPAT	OR	ON	2017/07/06 21:22
L16	10100	(G06F21/32 OR G06F21/34).cpc.	US-PGPUB; USPAT	OR	ON	2017/07/06 21:23
L17	37	L13 L16	US-PGPUB; USPAT	AND	ON	2017/07/06 21:23
L18	67	L14 OR L15 OR L17	US-PGPUB; USPAT	AND	ON	2017/07/06 21:23
L19	42	L18 @ad<"20140828"	US-PGPUB; USPAT	AND	ON	2017/07/06 21:24
L20	39	L19 (recognition)	US-PGPUB; USPAT	AND	ON	2017/07/06 21:24
L21	10	L19 (path or direction or line)near5(parameter or moving or movement)same(screen or area)	US-PGPUB; USPAT	AND	ON	2017/07/06 21:25
L22	18	L20 (path or direction or line or face or facial)near5(parameter or moving or movement or recognition or screen or area).clm.(authenticat$4).clm.	US-PGPUB; USPAT	AND	ON	2017/07/06 21:26
L23	22	L21 OR L22	US-PGPUB; USPAT	AND	ON	2017/07/06 21:26
L24	19	L23(authenticat$4).ab.(image or picture).clm. (face)	US-PGPUB; USPAT	AND	ON	2017/07/06 21:26
L25	4	L24(area or size)same(screen or display$4 or prompt$4 or different)same(face or image or picture)same(path or movement or moving or plac$4 or mov$3 or distance)same(user or camera or device).clm.	US-PGPUB; USPAT	AND	ON	2017/07/06 21:26
L26	7	L24(area or size)same(screen or display$4 or prompt$4 or different)same(face or image or picture)same(movement or moving or plac$4)same(direction or path or line or mov$3 or distance)same(user or camera or device)	US-PGPUB; USPAT	AND	ON	2017/07/06 21:27
L27	11	L25 OR L26	US-PGPUB; USPAT	AND	ON	2017/07/06 21:27
L28	6	L27(authenticat$4).ab.(image or picture).clm. (face or facial)same(recognition or movement).clm.	US-PGPUB; USPAT	AND	ON	2017/07/06 21:28
L29	6	L28(area or size)same(screen or display$4)	US-PGPUB;	AND	ON	2017/07/06 21:29

			USPAT			
L30	3	L28(area)same(screen)same(size or display$4)	US-PGPUB; USPAT	AND	ON	2017/07/06 21:29
L31	2	L28(threshold).clm.	US-PGPUB; USPAT	AND	ON	2017/07/06 21:29
L32	5	L30 OR L31	US-PGPUB; USPAT	AND	ON	2017/07/06 21:29
L34	2	L32 NOT L15	US-PGPUB; USPAT	AND	ON	2017/07/06 21:30
L35	5	L32 (user or authenticated or account or identifier).clm.	US-PGPUB; USPAT	AND	ON	2017/07/06 21:32
L36	4	L32 (user or account or identifier)same(authenticat$4 or stored).clm.	US-PGPUB; USPAT	AND	ON	2017/07/06 21:33
L37	1	L27(device)near3(identifier or serial)	US-PGPUB; USPAT	AND	ON	2017/07/06 21:35
L38	8	L27(area)same(screen)same(size or display$4)	US-PGPUB; USPAT	AND	ON	2017/07/06 21:37
L39	1	14/839505	US-PGPUB; USPAT	AND	ON	2017/07/06 21:39
L40	1	L39(area)same(screen)same(size or display$4)	US-PGPUB; USPAT	AND	ON	2017/07/06 21:39
L41	2	L27(area)same(screen)same(size or display$4 or position$4)same(face)	US-PGPUB; USPAT	AND	ON	2017/07/06 21:40
L42	0	L27(area)same(screen)same(size or display$4 or position$4)same(face).clm.	US-PGPUB; USPAT	AND	ON	2017/07/06 21:41
L43	1	L19(area)same(screen)same(size or display$4 or position$4)same(face).clm.	US-PGPUB; USPAT	AND	ON	2017/07/06 21:41
L44	1	L19(area)same(screen or prompt$4)same(size or display$4 or position$4)same(face).clm.	US-PGPUB; USPAT	AND	ON	2017/07/06 21:41
L45	0	L19(area)same(screen or prompt$4)same(size or display$4 or position$4)same(face).clm.(identifier or serial).clm.	US-PGPUB; USPAT	AND	ON	2017/07/06 21:41

7/6/2017 9:42:24 PM
C:\Users\sabedin\Documents\EAST\Workspaces\14570611.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14839505	TUSSY, KEVIN ALAN
	Examiner	Art Unit
	SHANTO M ABEDIN	2436

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	07/10/2017								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	O								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								

Biometric **authentication** on a **mobile** device: a study of user effort, error and task disruption

S Trewin, C Swart, L Koved, J Martino, K Singh... - Proceedings of the 28th ..., 2012 - dl.acm.org
... Tapping an '**Authenticate**' button ac- tivated the **authentication screen** for the current ... questionnaire elicited background information including experience **authenticating** on **mobile** devices. ... informed consent, participants used six different forms of **authentication** action, presented ...
Cited by 79 Related articles All 5 versions Cite Save

A robust gaze **detection** method by compensating for **facial movements** based on corneal specularities

YJ Ko, EC Lee, KR Park - Pattern Recognition Letters, 2008 - Elsevier
... Pattern **Recognition** Letters. ... of rectangle which was composed of four specularities was considered in order to reduce gaze errors caused by **facial movements**. ... So, we compensated for errors caused by user's **facial movement** based on the analysis of the 3D relations between ...
Cited by 44 Related articles All 4 versions Cite Save

Sensor-assisted **facial recognition**: an enhanced biometric **authentication** system for smartphones

S Chen, A Pande, P Mohapatra - ... international conference on **Mobile** ..., 2014 - dl.acm.org
... impede the prevalence of **facial authentication** in **mobile** devices. ... upon regular **face recognition** techniques that focus on **recognition** of **facial** features to identify and **authenticate** a person ... If no **face** is detected, the **authentication** system will show a prompt and ask the user to ...
Cited by 25 Related articles All 7 versions Cite Save

Facial recognition system for security access and identification

JS Coffin, D Ingram - US Patent 5,991,429, 1999 - Google Patents
... **Authentication** system for identification documents. US6950536, Sep 6, 2002, Sep 27, 2005, Houvener Robert C, High volume **mobile** identity verification system and method using tiered ... Fingerprint verification system utilizing a **facial** image-based heuristic search method. ...
Cited by 245 Related articles All 2 versions Cite Save

Personal **authentication** apparatus and personal **authentication** method

M Doi - US Patent 7,412,081, 2008 - Google Patents
... amount of the person of interest; and a unit configured to **authenticate** the person of ... Of America Corporation, Retrieving product information from embedded sensors via **mobile** device video ... 7, 2009, Feb 10, 2011, At&T Intellectual Property I, LP, Enhanced Biometric **Authentication**. ...
Cited by 40 Related articles All 3 versions Cite Save

Towards **face** unlock: on the difficulty of reliably detecting **faces** on **mobile** phones

RD Findling, R Mayrhofer - ... Conference on Advances in **Mobile** ..., 2012 - dl.acm.org
... video surveillance, but is now becoming a highly attractive alternative for **authenticating** users to ... assume a significantly higher difficulty level for tricking the system into **authentication** when rely ... below-the-phase camera **positions** due to the typical **position** of **mobile** phones when ...
Cited by 16 Related articles All 8 versions Cite Save

Understanding OSN-based **facial** disclosure against **face authentication** systems

Y Li, K Xu, Q Yan, Y Li, RH Deng - ... of the 9th ACM symposium on ..., 2014 - dl.acm.org
... A **mobile** system is usually more tolerant to varied en- vironments, as it should be ... ex- isting **face authentication** systems [1], where a participant should not pass user **authentication** if rotH ... researchers then removes the helmet gently and quickly in order to avoid **movement** of the ...
Cited by 23 Related articles All 2 versions Cite Save

Face liveness **detection** by exploring multiple scenic clues
J Yan, Z Zhang, Z Lei, D Yi, SZ Li - ... Automation Robotics & ..., 2012 - ieeexplore.ieee.org
... By using surveillance cameras in the public, digital cameras and **mobile** phones, or just Google ... Non-rigid motion analysis extracts information of local **facial movement**; **face**-background consistency analysis reveals ... Liveness verification in audio-video speaker **authentication**. ...
Cited by 53 Related articles All 9 versions Cite Save

Face recognition system
M Turk, AP Pentland - US Patent 5,164,992, 1992 - Google Patents
... 2000, Fraunhofer Gesellschaft Fuer Angewandte Forschung EV Et Al, Person identification based on **movement** information. ... US6185316, Nov 12, 1997, Feb 6, 2001, Unisys Corporation, Self-**authentication** apparatus and method. ... Real-time **facial recognition** and verification system ...
Cited by 359 Related articles All 2 versions Cite Save

System and method for providing secure access to an electronic device using **facial** biometric identification and **screen** gesture
C Azar, G Brostoff - US Patent App. 13/737,501, 2013 - Google Patents
... Many electronic devices such as personal computers, **mobile** devices including **mobile** phones and ... The user **authentication** apparatus includes a password input unit which determines whether a ... could be supplemented with a hidden action to either fully **authenticate** the user or ...
Cited by 11 Related articles All 2 versions Cite Save

Non-intrusive liveness **detection** by **face images**

K Kollreider, H Fronthaler, J Bigun - **Image** and Vision Computing, 2009 - Elsevier

... A poorly investigated problem in **face authentication** studies is the claim of someone else's identity by using a high ... Normal velocity in 2D xt- and yt-**images**: the plane in Fig ... If we have vertical and horizontal lines separately throughout the **image** sequence (achieved by directional ...

Cited by 119 Related articles All 14 versions Cite Save

Image reading apparatus and method for successively reading a plurality of partial **images** from a relatively **moving** object

Y Abiko - US Patent 8,358,870, 2013 - Google Patents

... from steps S31 to S33 not for the partial **image** but for the extended **image** so as to ... of times of repetition depends on the allowable width of a gap between the partial **images**. ... such as False Rejection Rate and False Acceptance Rate, in the personal **authentication** using output ...

Cited by 49 Related articles All 5 versions Cite Save

Estimating **face** orientation from robust **detection** of salient **facial** structures

N Gourier, D Hall, JL Crowley - FG Net Workshop on Visual ..., 2004 - venus.inrialpes.fr

... the real and the estimated horizontal angle has been computed for all 1395 **images** of fifteen ... angle is hard to estimate with only one eye visible on the **image** and that ... Conf. on Audio- and Videobased Bio- metric Person **Authentication**, Lecture Notes in Computer Science 1997. ...

Cited by 387 Related articles All 16 versions Cite Save More

Quantifying and **recognizing** human **movement** patterns from monocular video **images**-part ii: applications to biometrics

RD Green, L Guan - IEEE Transactions on Circuits and Systems ..., 2004 - ieeexplore.ieee.org

... QUANTIFYING AND **RECOGNIZING** HUMAN **MOVEMENT** PATTERNS FROM MONOCULAR VIDEO **IMAGES**—PART II ... L. Guan, and JA Burne, "An automated form of video **image** analysis applied ... Audio and Video-Based Bio- metric Person **Authentication**, Washington, DC, Mar ...

Cited by 52 Related articles All 14 versions Cite Save

Facial image recognition apparatus

H Dobashi, T Hirasawa, A Okazaki, T Sato... - US Patent ..., 2005 - Google Patents

... section which interrupts an infrared wavelength region of natural light, wherein the motion **picture** camera has a ... 14 shows display **screens** 110C, 110D, 110E as display examples of **facial images**. ... 14 , the **size** of the **facial image** at the time of the registration is represented by a ...

Cited by 50 Related articles All 4 versions Cite Save

Finger **movement detection** method and apparatus

S Nishikawa - US Patent 7,064,743, 2006 - Google Patents

... is obtained based on a displacement of the areas where the fingerprint **images** thereof agree ... 26, 2011, Nov 26, 2013, Validity Sensors, System for and method of **image** reconstruction with ... sensor by performance of a replication of a portion of an **authentication** process performed ...

Cited by 55 Related articles All 4 versions Cite Save

Is a **picture** really worth a thousand words? Exploring the feasibility of graphical **authentication** systems

A De Angeli, L Coventry, G Johnson... - International journal of ..., 2005 - Elsevier

... All of the graphical prototypes displayed detailed, colourful and meaningful **photos** of objects and scenes ... **Images** in the database were clustered into 9 semantic categories according to the subject ... Each **image** in the **authentication** code belonged to a different category and the ...

Cited by 257 Related articles All 21 versions Cite Save

Touchpad providing **screen** cursor/pointer **movement** control

A Ferrari, M Tartagni - US Patent 6,392,636, 2002 - Google Patents

... 18 is moved, or pitched, end to end on the horizontal upper surface of array 301, this **movement** being indicated by ... 1, the two-dimensional (2D) electronic signal-**picture**, output, or pattern of array 3, which encodes the touching function of ... Apparatus for **recognizing** an **image**. ...

Cited by 200 Related articles All 2 versions Cite Save

Sensor-assisted **facial recognition**: an enhanced biometric **authentication** system for smartphones

S Chen, A Pande, P Mohapatra - Proceedings of the 12th annual ..., 2014 - dl.acm.org

... The **images** taken from left and right will show different sides of the nose. **...** To achieve this goal, the key is to utilize smartphones' motion sensors and capture users' **face image** cleverly. **...** So far we have discussed how to quickly differentiate a real 3D **face** from a 2D **photo** (or video **...**

Cited by 25 Related articles All 7 versions Cite Save

Personal **authentication** apparatus and personal **authentication** method

M Doi - US Patent 7,412,081, 2008 - Google Patents

... US5446515 *, Jan 29, 1991, Aug 29, 1995, Wolfe; Maynard F. Automatic **picture** taking machine. **...** 2012, May 13, 2014, Bank Of America Corporation, Real-time video **image** analysis for **...** Jan 1, 2012, Aug 19, 2014, Bank Of America Corporation, **Recognizing** financial document **images ...**

Cited by 40 Related articles All 3 versions Cite Save

IEEE.org | IEEE *Xplore* Digital Library | IEEE-SA | IEEE Spectrum | More Sites Cart (0) | Create Account | Personal Sign In

Access provided by:
United States Patent and Trademark Office
Sign Out

BROWSE | MY SETTINGS | GET HELP | WHAT CAN I ACCESS?

Displaying results 1-4 of 4 for
((((("Abstract":authentication) AND facial recognition) AND movement) AND path) AND screen) AND area) and refined by
Year: 1990-2014

Show All Results Sort By Relevance

Select All on Page Download PDFs | Export | Set Search Alerts | Search History

Refine results by

Search within results

Content Type

- Books & eBooks (2)
- Conference Publications (2)

Year

Single Year | Range

1936 2010

From 1999 To 2010

Author

Affiliation

Publication Title

Publisher

Conference Location

1. **IP Security**
   Salah Aidarous; Thomas Plevyak; Paul Levine; Joberto Martins; Burkhard Stiller; Mostafa Hashem Sherif; Andrea Fumagalli; Javier Aracil; Luca Valcarenghi
   Managing IP Networks:Challenges and Opportunities
   Year: 2003
   Pages: 211 - 286, DOI: 10.1002/0471722987.ch5
   Wiley-IEEE Press eBook Chapters
   Abstract

2. **Proceedings 2003 International Conference on Multimedia and Expo (Cat. No.03TH8698)**
   Multimedia and Expo, 2003. ICME '03. Proceedings. 2003 International Conference on
   Year: 2003, Volume: 2
   Page: I, DOI: 10.1109/ICME.2003.1221537
   IEEE Conference Publications
   Abstract (2147 Kb)

3. **Biometric recognition in telecom environment**
   Ivan Krevatin
   2010 14th International Conference on Intelligence in Next Generation Networks
   Year: 2010
   Pages: 1 - 6, DOI: 10.1109/ICIN.2010.5640936
   IEEE Conference Publications
   Abstract (185 Kb)

   Modern telecom environment provides a rich set of services that require secure and reliable authentication. Biometric recognition is the only authentication technique that relies on person's characteristics for personal authentication. This paper gives an overview of a biometric system and biometric recognition techniques that use characteristics that are most suitabl... View more

4. **Secure Digital Payments**
   J Christopher Westland; Theordore H. Clark
   Global Electronic Commerce:Theory and Case Studies
   Year: 1999
   Pages: 465 - 528
   MIT Press eBook Chapters
   Abstract

IEEE Account
» Change Username/Password
» Update Address

Purchase Details
» Payment Options
» Order History
» View Purchased Documents

Profile Information
» Communications Preferences
» Profession and Education
» Technical Interests

Need Help?
» **US & Canada:** +1 800 678 4333
» **Worldwide:** +1 732 981 0060
» Contact & Support

About IEEE *Xplore* | Contact Us | Help | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.
© Copyright 2017 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

IEEE.org | IEEE *Xplore* Digital Library | IEEE-SA | IEEE Spectrum | More Sites Cart (0) | Create Account | Personal Sign In

Access provided by:
United States Patent and Trademark Office
Sign Out

BROWSE | MY SETTINGS | GET HELP | WHAT CAN I ACCESS?

Displaying results 1-5 of 5 for

(((((("Abstract":authentication) AND facial recognition) AND movement) AND parameter) AND image) distance enrollment mobile face area direction

and refined by

Year: 1990-2014

Show All Results Sort By Relevance

Select All on Page Download PDFs | Export | Set Search Alerts | Search History

Refine results by

Search within results

Content Type

- Journals & Magazines (3)
- Conference Publications (2)

Year

Single Year | Range

2004 2014

From 2004 To 2014

Author

Affiliation

Publication Title

Conference Location

Multi-modal biometrics for mobile authentication
Hagai Aronowitz; Min Li; Orith Toledo-Ronen; Sivan Harary; Amir Geva; Shay Ben-David; Asaf Rendel; Ron Hoory; Nalini Ratha; Sharath Pankanti; David Nahamoo
IEEE International Joint Conference on Biometrics
Year: 2014
Pages: 1 - 8, DOI: 10.1109/BTAS.2014.6996269
Referenced in: IEEE Biometrics Compendium, IEEE RFID Virtual Journal, IEEE RFID Virtual Journal
Cited by: Papers (5) | Patents (1)
IEEE Conference Publications

Abstract (547 Kb)

Authentication gets personal with biometrics
J. Ortega-Garcia; J. Bigun; D. Reynolds; J. Gonzalez-Rodriguez
IEEE Signal Processing Magazine
Year: 2004, Volume: 21, Issue: 2
Pages: 50 - 62, DOI: 10.1109/MSP.2004.1276113
Cited by: Papers (53)
IEEE Journals & Magazines

Abstract (761 Kb)

An integrated vision-based architecture for home security system
John See; Sze-Wei Lee
IEEE Transactions on Consumer Electronics
Year: 2007, Volume: 53, Issue: 2
Pages: 489 - 498, DOI: 10.1109/TCE.2007.381720
Cited by: Papers (9)
IEEE Journals & Magazines

Abstract (508 Kb)

Biometric recognition in telecom environment
Ivan Krevatin
2010 14th International Conference on Intelligence in Next Generation Networks
Year: 2010
Pages: 1 - 6, DOI: 10.1109/ICIN.2010.5640936
IEEE Conference Publications

Abstract (185 Kb)

IEEE.org | IEEE *Xplore* Digital Library | IEEE-SA | IEEE Spectrum | More Sites Cart (0) | Create Account | Personal Sign In

Access provided by:
United States Patent and Trademark Office
Sign Out

BROWSE MY SETTINGS GET HELP WHAT CAN I ACCESS?

Displaying results 1-6 of 6 for

(((((("Abstract":authentication) AND facial recognition) AND movement) AND parameter) AND image) distance enrollment mobile face area

and refined by

Year: 1990-2014

Show All Results Sort By Relevance

Select All on Page Download PDFs | Export | Set Search Alerts | Search History

Refine results by

Search within results

Content Type

- Conference Publications (3)
- Journals & Magazines (3)

Year

Single Year | Range

2004 2014

From 2004 To 2014

Author

Affiliation

Publication Title

Conference Location

1. **Multi-modal biometrics for mobile authentication**
   Hagai Aronowitz; Min Li; Orith Toledo-Ronen; Sivan Harary; Amir Geva; Shay Ben-David; Asaf Rendel; Ron Hoory; Nalini Ratha; Sharath Pankanti; David Nahamoo
   IEEE International Joint Conference on Biometrics
   Year: 2014
   Pages: 1 - 8, DOI: 10.1109/BTAS.2014.6996269
   Referenced in: IEEE Biometrics Compendium, IEEE RFID Virtual Journal, IEEE RFID Virtual Journal
   Cited by: Papers (5) | Patents (1)
   IEEE Conference Publications
   Abstract (547 Kb)

2. **Authentication gets personal with biometrics**
   J. Ortega-Garcia; J. Bigun; D. Reynolds; J. Gonzalez-Rodriguez
   IEEE Signal Processing Magazine
   Year: 2004, Volume: 21, Issue: 2
   Pages: 50 - 62, DOI: 10.1109/MSP.2004.1276113
   Cited by: Papers (53)
   IEEE Journals & Magazines
   Abstract (761 Kb)

3. **Revolution in authentication process by using biometrics**
   Arundhuti Chowdhury
   2011 International Conference on Recent Trends in Information Systems
   Year: 2011
   Pages: 36 - 41, DOI: 10.1109/ReTIS.2011.6146836
   IEEE Conference Publications
   Abstract (794 Kb)

4. **An integrated vision-based architecture for home security system**
   John See; Sze-Wei Lee
   IEEE Transactions on Consumer Electronics
   Year: 2007, Volume: 53, Issue: 2
   Pages: 489 - 498, DOI: 10.1109/TCE.2007.381720
   Cited by: Papers (9)
   IEEE Journals & Magazines
   Abstract (508 Kb)

☐ **Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication**
Mario Frank; Ralf Biedert; Eugene Ma; Ivan Martinovic; Dawn Song
IEEE Transactions on Information Forensics and Security
Year: 2013, Volume: 8, Issue: 1
Pages: 136 - 146, DOI: 10.1109/TIFS.2012.2225048
Referenced in: IEEE Biometrics Compendium, IEEE RFID Virtual Journal, IEEE RFID Virtual Journal
Cited by: Papers (125) | Patents (4)
IEEE Journals & Magazines

Abstract (1709 Kb)

« First < 1 > Last »

IEEE Account
» Change Username/Password
» Update Address

Purchase Details
» Payment Options
» Order History
» View Purchased Documents

Profile Information
» Communications Preferences
» Profession and Education
» Technical Interests

Need Help?
» **US & Canada:** +1 800 678 4333
» **Worldwide:** +1 732 981 0060
» Contact & Support

About IEEE *Xplore* | Contact Us | Help | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.
© Copyright 2017 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

IEEE.org | IEEE *Xplore* Digital Library | IEEE-SA | IEEE Spectrum | More Sites Cart (0) | Create Account | Personal Sign In

Access provided by:
United States Patent and Trademark Office
Sign Out

BROWSE | MY SETTINGS | GET HELP | WHAT CAN I ACCESS?

Displaying results 1-5 of 5 for

(((((("Abstract":authentication) AND facial recognition) AND movement) AND parameter) AND image) distance enrollment mobile face parameter screen

and refined by

Year: 1990-2014

Show: All Results | Sort By: Relevance

Select All on Page | Download PDFs | Export | Set Search Alerts | Search History

Refine results by

Search within results

Content Type

- Conference Publications (4)
- Journals & Magazines (1)

Year

Single Year | Range

2010 2014

From: 2010 To: 2014

Author

Affiliation

Publication Title

Conference Location

1. **Multi-modal biometrics for mobile authentication**
   Hagai Aronowitz; Min Li; Orith Toledo-Ronen; Sivan Harary; Amir Geva; Shay Ben-David; Asaf Rendel; Ron Hoory; Nalini Ratha; Sharath Pankanti; David Nahamoo
   IEEE International Joint Conference on Biometrics
   Year: 2014
   Pages: 1 - 8, DOI: 10.1109/BTAS.2014.6996269
   Referenced in: IEEE Biometrics Compendium, IEEE RFID Virtual Journal, IEEE RFID Virtual Journal
   Cited by: Papers (5) | Patents (1)
   IEEE Conference Publications
   Abstract (547 Kb)

2. **FAME: Face Authentication for Mobile Encounter**
   Silvio Barra; Maria De Marsico; Chiara Galdi; Daniel Riccio; Harry Wechsler
   2013 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications
   Year: 2013
   Pages: 1 - 7, DOI: 10.1109/BIOMS.2013.6656140
   Cited by: Papers (2)
   IEEE Conference Publications
   Abstract (581 Kb)

3. **SAFE: Secure authentication with Face and Eyes**
   Arman Boehm; Dongqu Chen; Mario Frank; Ling Huang; Cynthia Kuo; Tihomir Lolic; Ivan Martinovic; Dawn Song
   2013 International Conference on Privacy and Security in Mobile Systems (PRISMS)
   Year: 2013
   Pages: 1 - 8, DOI: 10.1109/PRISMS.2013.6927175
   Cited by: Papers (1) | Patents (1)
   IEEE Conference Publications
   Abstract (2098 Kb)

4. **Biometric recognition in telecom environment**
   Ivan Krevatin
   2010 14th International Conference on Intelligence in Next Generation Networks
   Year: 2010
   Pages: 1 - 6, DOI: 10.1109/ICIN.2010.5640936

Referenced in: IEEE Biometrics Compendium, IEEE RFIC Virtual Journal, IEEE RFID Virtual Journal
Cited by: Papers (125) | Patents (4)
IEEE Journals & Magazines

Abstract (1709 Kb)

« First < 1 > Last »

IEEE Account	Purchase Details	Profile Information	Need Help?
» Change Username/Password	» Payment Options	» Communications Preferences	» **US & Canada:** +1 800 678 4333
» Update Address	» Order History	» Profession and Education	» **Worldwide:** +1 732 981 0060
	» View Purchased Documents	» Technical Interests	» Contact & Support

About IEEE *Xplore* | Contact Us | Help | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.
© Copyright 2017 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2003/0095053	05/03	Kandogan			
		2006/0224523	10/06	Elvitigala			
		2014/0022179	01/14	Yoon			
		2014/0173443	06/14	Hawkins, III			
		2014/0337791	11/14	Agnetta			
		2014/0351761	11/14	Bae			
		2015/0074615	03/15	Han			
		2015/0148106	05/15	Choi			
		2015/0205399	07/15	Kim			
		2015/0205454	07/15	Ainslie			
		2015/0212684	07/15	Sabia			
		2015/0227286	08/15	Kang			
		2016/0026425	01/16	Lee			
		D596192	07/09	Shotel			
		D601582	10/09	Chaudhri			
		D625325	10/10	Vu			
		D640277	06/11	Woo			
		D692018	10/13	Wenz			
		D702714	04/14	Abratowski			
		D715317	10/14	Pearce			
		D717339	11/14	Wen			
		D725151	03/15	Bray			
		D725668	03/15	Clare			
		D728623	05/15	Lim			
		D730389	05/15	Izotov			
		D730941	06/15	Marianek			

EXAMINER /SHANTO ABEDIN/	DATE CONSIDERED 07/13/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.A/

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT (USE SEVERAL SHEETS IF NECESSARY)	INVENTOR(S) Kevin Alan Tussy	
	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		D731552	06/15	Seo			
		D733755	07/15	Kadosh			
		D736812	08/15	Yoo			
		D738921	09/15	Lim			
		D740833	10/15	Bae			
		D742417	11/15	Brunner			
		D745567	12/15	Park			
		D747354	01/16	Park			

EXAMINER INITIAL		**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)
		Rogssignol, Joe. "How to customise the Lock screen in iOS 7." iDownloadBlog, posted January 11, 2014 (Retrieved from the internet 3/30/2016). Internet URL: <http: //www.idownloadblog.com/2014/01/11/how-to-theme-the-lock-screen-on-oos-7/>
		android_locked-out-PDF, screenshot, date unknown, author unknown.
		android-lock-screen1-PDF, screenshot, date unknown, author unknown.
		facetime-PDF, screenshot, date unknown, author unknown.
		image 9-PDF, screenshot, date unknown, author unknown.
		iphone-Facetime-PDF, screen shot, date unknown, author unknown.
		keyboard-PDF, screen shot, date unknown, author unknown.
		passcode-lock-PDF, screen shot, date unknown, author unknown.
		passcode-PDF, screen shot, date unknown, author unknown.
		screen Shot-PDF, screen shot, date unknown, author unknown.
		screenshot_2012-06-20-16-06-32-PDF, screen shot, date unknown, author unknown.
		topic_facetime_ios-PDF, screen shot, date unknown, author unknown.
		wp_ss_20130124_00071-PDF, screen shot, January 24, 2013, author unknown.
		Shutterstock [online], 4 August 2014 [retried 24 July 2016]. Retrieved from the internet URL:http://www.tineye.com/search/543afefb8836762927558call587ce7f99a706ad/.,pic-199246373 stock phot male silhouette image.

EXAMINER	/SHANTO ABEDIN/	DATE CONSIDERED	07/13/2017

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2003/0095053	05/03	Kandogan			
		2006/0224523	10/06	Elvitigala			
		2014/0022179	01/14	Yoon			
		2014/0173443	06/14	Hawkins, III			
		2014/0337791	11/14	Agnetta			
		2014/0351761	11/14	Bae			
		2015/0074615	03/15	Han			
		2015/0148106	05/15	Choi			
		2015/0205399	07/15	Kim			
		2015/0205454	07/15	Ainslie			
		2015/0212684	07/15	Sabia			
		2015/0227286	08/15	Kang			
		2016/0026425	01/16	Lee			
		D596192	07/09	Shotel			
		D601582	10/09	Chaudhri			
		D625325	10/10	Vu			
		D640277	06/11	Woo			
		D692018	10/13	Wenz			
		D702714	04/14	Abratowski			
		D715317	10/14	Pearce			
		D717339	11/14	Wen			
		D725151	03/15	Bray			
		D725668	03/15	Clare			
		D728623	05/15	Lim			
		D730389	05/15	Izotov			
		D730941	06/15	Marianek			

EXAMINER	DATE CONSIDERED

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2436

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		D731552	06/15	Seo			
		D733755	07/15	Kadosh			
		D736812	08/15	Yoo			
		D738921	09/15	Lim			
		D740833	10/15	Bae			
		D742417	11/15	Brunner			
		D745567	12/15	Park			
		D747354	01/16	Park			

EXAMINER INITIAL		**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)
		Rogssignol, Joe. "How to customise the Lock screen in iOS 7." iDownloadBlog, posted January 11, 2014 (Retrieved from the internet 3/30/2016). Internet URL: <http: //www.idownloadblog.com/2014/01/11/how-to-theme-the-lock-screen-on-oos-7/>
		android_locked-out-PDF, screenshot, date unknown, author unknown.
		android-lock-screen1-PDF, screenshot, date unknown, author unknown.
		facetime-PDF, screenshot, date unknown, author unknown.
		image 9-PDF, screenshot, date unknown, author unknown.
		iphone-Facetime-PDF, screen shot, date unknown, author unknown.
		keyboard-PDF, screen shot, date unknown, author unknown.
		passcode-lock-PDF, screen shot, date unknown, author unknown.
		passcode-PDF, screen shot, date unknown, author unknown.
		screen Shot-PDF, screen shot, date unknown, author unknown.
		screenshot_2012-06-20-16-06-32-PDF, screen shot, date unknown, author unknown.
		topic_facetime_ios-PDF, screen shot, date unknown, author unknown.
		wp_ss_20130124_00071-PDF, screen shot, January 24, 2013, author unknown.
		Shutterstock [online], 4 August 2014 [retried 24 July 2016]. Retrieved from the internet URL:http://www.tineye.com/search/543afefb8836762927558call587ce7f99a706ad/.,pic-199246373 stock phot male silhouette image.

EXAMINER	DATE CONSIDERED

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

CWM-W-11732

Electronic Acknowledgement Receipt

EFS ID:	28521293
Application Number:	14839505
International Application Number:	
Confirmation Number:	6236
Title of Invention:	Facial Recognition Authentication System Including Path Parameters
First Named Inventor/Applicant Name:	Kevin Alan Tussy
Customer Number:	32856
Filer:	Chad W. Miller
Filer Authorized By:	
Attorney Docket Number:	FACIAL.0012P
Receipt Date:	02-MAR-2017
Filing Date:	28-AUG-2015
Time Stamp:	19:24:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	CWMW11733TRANS.pdf	84827 85861f7dd7169b6e61eb9ac195b4c0810798910c	no	1

Warnings:

Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	CWMW11732PTO1449.pdf	94390 fccbead7668183b89e913f19286cedc8fe4cbc4e	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Non Patent Literature	REF1ROGSSIGNOL.pdf	1346214 2d639d084f34a906d7c2b6406a089b06adba2ff4	no	4
Warnings:					
Information:					
4	Non Patent Literature	REF2androidlockedoutPDF.pdf	126682 86fd39237e369a43bafb497681a55738579d94e6	no	1
Warnings:					
Information:					
5	Non Patent Literature	REF3androidlockscreen1PDF.pdf	357822 db4565b0e811eea91a712cc92ecbdc57775fec3d	no	1
Warnings:					
Information:					
6	Non Patent Literature	REF4facetimePDF2.pdf	704788 afc0819071dfb0d02ca1948e59dff78fd5a29b58	no	1
Warnings:					
Information:					
7	Non Patent Literature	REF5image9PDF.pdf	44982 86dac3d9822823d6a62571b861342a1e92b0f137	no	1
Warnings:					
Information:					
8	Non Patent Literature	REF6iphoneFacetimePDF2.pdf	636230 95a856cda0b83c1527f4b3889f33b83a67645b8e	no	1
Warnings:					
Information:					

9	Non Patent Literature	REF7keyboardPDF2.pdf	867687 6f67af52de8bf8106d4cc1045f49ae623811ea37	no	1
Warnings:					
Information:					
10	Non Patent Literature	REF8passcodelockPDF.pdf	92641 f280e90eeae916478a361c9d3ffccba0fe73242b	no	1
Warnings:					
Information:					
11	Non Patent Literature	REF9passcodePDF.pdf	105836 095652321a53cdd6cf662cf8d2eb6e8ed8529490	no	1
Warnings:					
Information:					
12	Non Patent Literature	REF10screenshotPDF.pdf	271950 5b2f052c76883ed521abaf623e9f754ce097e7f5	no	1
Warnings:					
Information:					
13	Non Patent Literature	REF11screenshot20120620160632PDF.pdf	259196 337df3ef48b8eac82e57256c627c29edc5e9b599	no	1
Warnings:					
Information:					
14	Non Patent Literature	REF12topicfacetimeiosPDF2.pdf	645151 89670bd0eb0ded68a0b3a00f30aabfec704eef5b	no	1
Warnings:					
Information:					
15	Non Patent Literature	REF13wpss2013012400071PDF.pdf	49869 5971474a1eb9f58ca1ab5dc690f84525118b4146	no	1
Warnings:					
Information:					

16	Non Patent Literature	REF14ShutterstcokOnlinetTiney e.pdf	396893 a09c3b6843aa1cde750c282f3fe1dff35fdfe 01e	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	6085158	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

FACIAL.0012P PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s)	:	Kevin Alan Tussy
App. No.	:	14/839,505
Filed	:	August 28, 2015
For	:	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS
Examiner	:	Shanto Abedjin

Group Art Unit: 2436

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Patent and Trademark Office via EFSWeb, on:

March 2, 2017
(Date)

/Chad W. Miller/
Chad W. Miller, Reg. No. 44,943

SECOND SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Enclosed is form PTO-1449 listing 34 U.S. references, copies of which are not required to be provided in accordance with 37 C.F.R. §1.98(e), and 14 publications, copies of which are enclosed herewith. This Information Disclosure Statement is being filed before the mailing of the first Office Action on the merits, and as such, no fee is required in accordance with 37 C.F.R. §1.97(b)(3).

Respectfully submitted,

Dated: March 2, 2017

By: /Chad W. Miller/
Chad W. Miller
Attorney for Applicant
Weide & Miller, Ltd.
Registration No. 44,943
7251 W. Lake Mead Blvd., Suite 530
Las Vegas, NV 89128
Tel. (702) 382-4804 (Pacific Time)
cmiller@weidemiller.com

CWM-W-11733

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/839,505	08/28/2015	Kevin Alan Tussy	FACIAL.0012P

CONFIRMATION NO. 6236

32856
WEIDE & MILLER, LTD.
7251 W. LAKE MEAD BLVD.
SUITE 530
LAS VEGAS, NV 89128

PUBLICATION NOTICE

OC000000081130693

Title: Facial Recognition Authentication System Including Path Parameters

Publication No.US-2016-0063235-A1
Publication Date:03/03/2016

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2431

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		2012/0140993	06/12	Bruso, et al.			
		2014/0123275	05/14	Azar, et al.			

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO
		KR 20130097581	09/13	KR (abstract, description & claims translation only)			X	
		CN 103593594 2013	02/14	CN (abstract, description & claims translation only)			X	

EXAMINER INITIAL		**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)
		Girija Chetty and Michael Wagner, "Automated lip feature extraction for liveness verification in audio-video authentication", Human Computer Communication laboratory School of Information Sciences and Engineering, University of Canberra, Australia, Proc. Image and Vision Computer (2004), 1 January, 2004, 6 pages.

EXAMINER	DATE CONSIDERED

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

CWM-W-10610

Espacenet

Bibliographic data: KR20130097581 (A) — 2013-09-03

METHOD AND APPARATUS FOR AUTHENTICATING USER USING HYBRID BIOMETRICS INFORMATION IN A USER DEVICE

Inventor(s): KANG SANG KI [KR]; KIM KYUNG TAE [KR]; LEE SANG HOON [KR]; KIM YANG WOOK [KR]; LEE CHUL HWAN [KR]; JUNG SEOK YEONG [KR] ± (KANG, SANG KI, ; KIM, KYUNG TAE, ; LEE, SANG HOON, ; KIM, YANG WOOK, ; LEE, CHUL HWAN, ; JUNG, SEOK YEONG)

Applicant(s): SAMSUNG ELECTRONICS CO LTD [KR] ± (SAMSUNG ELECTRONICS CO., LTD)

Classification: **- international:** ***G06K9/20; G06K9/46***
- cooperative: **G06F21/32; G06K9/00335; G10L17/10;** G06K9/00892; G06K9/6293; G10L15/25

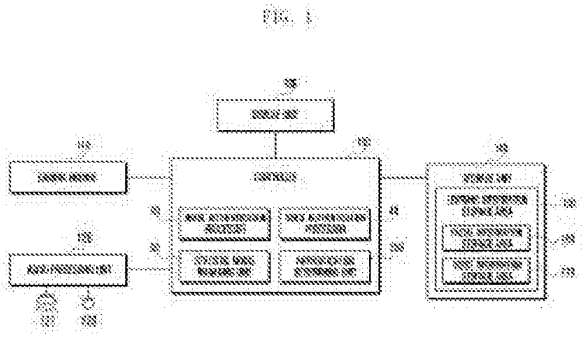
Application number: KR20120019333 20120224

Priority number(s): KR20120019333 20120224

Also published as: EP2631843 (A2) EP2631843 (A3) US2013227678 (A1) WO2013125910 (A1)

Abstract of KR20130097581 (A)

PURPOSE: A user authentication method using complex biometric information in a user device and a device thereof are provided to perform integral user authentication by additionally detecting the operational variation of a face, a mouth and an eye in a user authentication process using video authentication information and voice authentication information. CONSTITUTION: A video



authentication processing part (10) processes user authentication by detecting face characteristic vector and object characteristic vector from videos secured through a camera module (110). A voice authentication processing part (40) processes the user authentication by detecting the voice characteristic vector from a voice secured from a microphone. An authentication determining part (290) processes the integral authorization of a user based on the authentication information delivered from the video and voice authentication processing parts. A storing part (140) stores the statistical model for face recognition and the statistical model for voice recognition. [Reference numerals] (10) Video authentication processing part; (110) Camera module; (120) Audio processing part; (130) Display part; (140) Storing part; (160) Face information; (170) Voice information; (180) Control part; (290) Authentication determining part; (40) Voice authentication processing part; (50) Statistics module management part

Patent Translate
Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

DESCRIPTION KR20130097581

User devices in complex biometric information using the user authentication method and apparatus (METHOD AND APPARATUS FOR AUTHENTICATING USER USING HYBRID BIOMETRICS INFORMATION IN A USER DEVICE)

[0001]

[0001] How the present invention relates to a user authentication method and apparatus in a user device, in particular in the user device using the composite biometric information (hybrid biometrics information) such as a user of video information and audio information to authenticate the user and that to an apparatus.

[0002]

[0002] Recent digital technology development and with the mobile communication terminal, PDA (Personal Digital Assistant), an electronic organizer, a smart phone, a tablet PC (Personal Computer), etc. as moving while communicating and Privacy capable user devices variously released being. The user device is a voice call, SMS (Short Message Service) / MMS (Multimedia Message Service) such as sending a message, a video call, an electronic organizer, an up, e-mail transmission and reception, broadcast playback, video playback, Internet, e-commerce, music playback, such as calendars, social networking services (SNS, social Networking service), IM, dictionaries, games can be provided with various functions.

[0003]

[0003] On the other hand, there is a security feature is provided to prevent the indiscriminate use from the other user of the user device. For example, the user device turn-on (turn-on) during lock-screen (lock screen) support this function, such as to release the locking by the user of the set password (password) entered in the lock screen is provided, being. Recently, the user's fingerprint, face, voice, retina, and has been noted for the unique physical characteristics such as iris using biometric technology is a new user authentication system for its superior security reasons user authentication, and the use of the is a trend in increasing rapidly.

[0004]

[0004] On the other hand, biometrics enables user authentication by including user you need to close your eyes to the fingerprint reader iris reader input fingerprint information, or directly to the provided in the user device using the user's physical characteristics from the existing user device to impose specific actions for you to enter the information was somewhat

inconvenient input biometric information. On the other hand, in the case where the biometric information of the face information or audio information, there are advantages that can greatly reduce the inconvenience or discomfort a user feels when the input biometric information. Also it has the advantage of reducing the additional cost can utilize the camera module or a microphone provided in the user device without the need for an input device for biometric information as recognized separately. As a result, the biometric information of the user authentication technology through research on the face or voice recognition, among being more actively conducted.

An object of the present invention to provide a user authentication method and apparatus using a composite biometric information from the user device to implement the user authentication system. Another object of the present invention to provide a user authentication method and apparatus that can increase the security performance by the integrated user authentication based on the authentication image information and audio information from the user device authentication. It is another object of the present invention add an image authentication information and voice authentication information upon user authentication the face, mouth, changes in motion of the eye with the user device is detected to provide a user authentication method and apparatus that can perform an integrated user authentication it is on. Another object of the present invention is to provide a user authentication method and apparatus that determines further whether the user authentication with the lips motion and sound synchronization between using image authentication information and voice authentication information from the user device to perform an integrated user authentication have. Another object of the present invention is way in the authentication mode of the user device to enhance security for optimum environment to improve the performance of users' convenience by competitive usability and user device of the user device in accordance with user authentication, and device to provide for.

Method according to an embodiment of the present invention to achieve the objects as described above, in the process of the user authentication method, obtaining biometric information of two different for user authentication; Generating each of the plurality of authentication biometric information acquisition process; And generates the step of including an integrated user authentication based on the authentication information. In the embodiment of the present invention to achieve the objects as described above, it includes a computer-readable recording medium storing a program for executing the method on a processor. Generating each of the authentication information on the recording medium according to an embodiment of the invention, obtaining a plurality of different biometric information for user authentication, and acquired a plurality of biometric information to achieve the objects as described above and it includes a program to perform a single sign-on based on the generated authentication information. In the user device according to an embodiment of the present invention, to achieve the objects as described above, the camera module for acquiring the image; A microphone for acquiring a voice; And a control unit for processing a single sign-on user using a plurality of authentication information generated by the camera module and the microphone configured to obtain a plurality of different biometric information, based on the plurality of biometric information The. Information, as described above are the features and technical advantages of the present invention in order to be able better understood from the detailed description of the invention which will be described later in the art who has the knowledge usually is a little wider outline. In addition to these features, and advantages will be better understood from the detailed description of the present invention described below are additional features and advantages of the present invention that forms the subject of the claims of the present invention.

According to the user authentication method using a composite biometric information from the user device proposed by the present invention as described above, and devices, single biometrics to authenticate the user at the user device information (e.g., voice recognition, facial recognition) only than the method using It has the benefit of increasing security. According to the present invention, there is an advantage that enables a single sign-on using a complex biometric authentication information, such as face and voice information credentials. According to the invention, when the user authentication based on the image authentication information and voice authentication information from the user device, adding a motion change of the user authentication at the face, mouth, eye detection, add determines whether synchronization between the lips motion and sound by performing an integrated user authentication, the security performance and a user device it can be derived to be used by the legitimate user. According to the invention, a separate device for the user authentication (for example, sensors, etc.) which may utilize the camera module and the microphone provided in the user device, without having the. And the present invention can be implemented in a variety of devices that form all of a user device and corresponding thereto. In addition, it can contribute to implement an optimal environment for the user authentication from the user device according to the present invention, to improve the usability, convenience and competitiveness of the user device.

[0017]

[0017] Figure 1 is a view generally showing a structure of a user device according to an embodiment of the present invention. 2 to 4 is a diagram illustrating a configuration of a control unit in the embodiment; 5 is a diagram illustrating an exemplary operation for authenticating the user by using the composite biometric information from the user device according to an embodiment of the present invention. 6 is a flowchart illustrating a statistical model registration method for user authentication in the user device according to an embodiment of the present invention. 7 and 8 are a flowchart showing a user authentication method from the user device according to an embodiment of the present invention. 9 is a flowchart illustrating an operating method for user authentication in the user device according to an embodiment of the present invention.

[0018]

[0018] Hereinafter, with reference to the accompanying drawings will be described preferred embodiments of the present invention; In this case, the same components in the accompanying drawings shall be noted that designated by like reference numerals as possible. In the following description, a detailed description of known functions and configurations may blur the point of the present invention will be omitted. In other words, in the following description and description is only necessary for understanding the operations according to an embodiment of the invention section, the description of the other part is to be noted that there will be omitted so that the ridge heutteu matter of the present invention.

[0019]

[0019] In the following, with reference to to the structure and the operation control method of a user device according to an embodiment of the present invention a description will now be. It is the configuration and operation control method for a user device according to an embodiment of the invention is not limited to or limited to the contents described in the basis of the following examples not to be applied should be noted that in various embodiments. In the present invention described below will be described as an example the hardware approach. However, the present invention, because it contains a technology using both hardware and software, and are not intended to exclude the invention is a software-based approach.

[0020]

[0020] Figure 1 is a diagram schematically showing a configuration of user device 100 according to an embodiment of the present invention.

[0021]

[0021] Referring to FIG 1, the user device 100 of the present invention includes a camera module 110, the audio processing unit 120, display unit 130, storage unit 140, and controller 180 It is configured. In addition, the user device 100 is a digital broadcasting the digital broadcast module for the reception of the (e.g., DMB (Digital Multimedia Broadcasting) or DVB (Digital Video Broadcasting), digital multimedia broadcasting, such as), Bluetooth (Bluetooth) communication, infrared (IrDA, Infrared Data Association) communication, RFID (radio Frequency Identification) communication, and NFC (near Field communication) as such short-range wireless communication based on the communication function support for the at least one short-range communication module, a hard key (hard key) based on the input support wireless LAN (LAN, Local Area Network) for the vibration-generating unit, Internet service support for the wireless communication unit, a vibration generating for a communication function supported on the input, the mobile communication-based voice calls, video calls, data calls, and for the module, and above may further comprise a structure such as a battery (battery) for supplying power to the configuration, described and illustrated for them will be omitted.

[0022]

[0022] The above camera module 110 supports a static image and a dynamic image photographing of the subject. The camera module 110 is taken to any subject in accordance with the control of the controller 180, and transmits the photographed image data to the display unit 130 and the controller 180. The camera module 110 and the like with (not shown), a camera sensor for converting an input optical signal into an electrical signal, (not shown) signal processor for converting an electric signal inputted from the camera sensor into digital image data it can be configured. The camera sensor may include a sensor using a method such as CCD (Charge-Coupled Device) or CMOS (Complementary Metal-Oxide-Semiconductor). In particular, the camera module 110 in the present invention is driven under the control of the controller 180, the authentication mode is enabled for the user authentication, a static image and a dynamic image of the outside of the subject (e.g., user's face, etc.) up, and passes each of the image that is photographed by the controller 180.

[0023]

[0023] The audio processing unit 120 is configured to include a speaker (speaker) (121) and a microphone (microphone) (123), processes the input and output of the audio signal of the user device 100. For example, the audio processing unit 120 and sends audio signals received from the controller 180 to the speaker 121, an audio signal of a voice or the like received from the microphone 123 to the controller 180, it performs the function of transmission. The audio processing unit 120 is an audio signal of voice, etc. that receive voice / audio data from the microphone 123 according to the control, and outputs the converted audible sound through the speaker 121, the controller 180 digital is converted to a signal it can be passed to the controller 180. In particular, the audio processing unit 120 according to the present invention is under the control of the controller 180, the authentication mode for the user authentication of receiving a user's voice, the controller 180 converts the voice signal into a digital signal corresponding it is delivered to. And the audio processing unit 120 may output under the control of the controller 180 in the authentication mode, the feedback, such as user authentication process proceeds on success or failure of the sound effect to the speaker 121. Feedback on the success or failure of the authentication may be set to vary depending on each user setting.

[0024]

[0024] The display unit 130 may display the operating status and the associated screen of the user device 100. For example, the display unit 130 is the user device 100 of the lock screen (lock screen), the home screen (home screen), the menu screen (menu screen), the message composition screen, the chat screen, video playback, and a variety of it may display a screen such as each execution of the executable application. And the display 130 displays information which the user is provided to a user or information input, including various menus of the user device 100. That is, the display 130 may provide an execution screen of the various functions according to the user using the user device 100. The display 130 is a liquid crystal display device (LCD, Liquid Crystal Display) is used which is common or, the light emitting diode (LED, Light Emitting Diode), an organic light emitting diode (OLED, Organic LED), and the active matrix OLED (AMOLED, Active the other display devices such as Matrix OLED) can be used. In addition, the display 130 may be implemented in a flexible display (flexible display) to be bent. The flexible display device that shows a bent without damage via a thin, flexible substrates like paper, bend or be late. In addition, the display unit 130 may be configured to include an interface (interface) to support the touch (touch) of the based type. For example, the display unit 130 supports a variety of user input based on the touch by the touch screen (touchscreen) configuration, to generate an input signal according to a user input can be transmitted to the controller 180. In addition, the display unit 130 according to when to display various screens, such as the above user devices the direction of rotation (or lying direction) of 100 in the landscape screen display, the display screen according to the portrait mode and landscape mode and the portrait mode, it can support adaptive switching screen display according to the change between.

In particular, the display unit 130 may display a specific image provided in accordance with the control of the control unit 180 in the authentication mode for the user authentication of the user device 100. For example, the display unit 130 may display the user information of the face is photographed through the camera module 110 in the certification mode.

[0025]

[0025] may be configured to include the storage unit 140 the user device stores various applications and the data operating in the 100, one or more non-volatile memory (non-volatile memory) and volatile memory (volatile memory) have. The storage unit 140 has ROM (Read Only Memory), a flash memory (flash memory), RAM (Random Access Memory), an internal hard disk (HDD, Hard Disk), an external hard disk, a memory card (memory card), such as it may be comprised of at least one, such as an external storage medium. And the storage unit 140 using the user device 100 of the operating system, programs and data relating to the display control operation of the display section 130, the composite biometric information in the authentication mode (e.g., facial information and audio information) it can be continuously or temporarily store programs and data related to user operations such as authentication. In particular, the storage unit 140 may store each of the data relating to the video photographed by the camera module 110 in the authentication mode according to an embodiment of the present invention as a static data and dynamic data. And the storage unit 140 may store the learned information for identifying the biometric information input to the user authentication in the authentication mode in the learning information storage area 150. The learning information can be separated by a face information and audio information, it may be stored in each of the allocated storage area. The face information extracting a certain facial features in your video to be authenticated in the authentication mode, and the face based on the extracts the facial features characteristic vector (feature vector) created by saving face information into statistical models for face recognition zone (It may be registered in 160). The voice information registered in the audio information storage area (170) extracts a predetermined audio features from the user's speech, and generating a speech feature vector based on the extract the speech features to a statistical model for speech recognition to be authenticated in the authentication mode, it can be.

[0026]

[0026] Further, the storage unit 140 may include a program area and a data area. The program area may store an operation for a boot and operation of each configuration described above of the user device 100 and the system, downloaded and installed applications, and the like. The data region is a region to which the data is stored to occur depending on the use of the user device 100. Wherein the data area stores data used or generated according to the running application, it may be buffering or storing image data and voice data input at the authentication mode.

[0027]

[0027] The controller 180 controls the overall operation of the user device 100. In particular, the controller 180 may control the operations related to the user authentication using biometric information such as facial composite and audio information in the authentication mode of the user device 100. The controller 180 may process the integrated authentication for the user based on the complex information, such as face recognition results, a result of voice recognition, object determination result, and a synchronization judgment result in the authentication mode. Then, the controller 180 may determine an error for the user authentication information to be confirmed that the complex of any one of the unauthorized users also. For example, each of the results for notifying that predefined reference probability value (e.g., 80%, 85%, 90%, etc.) to meet whether the result notifying that the authenticated user output or non-authenticated user in response to that the results can be output. Therefore, the control unit 180 may over whether to meet the individual probabilities of each of the results to determine whether the error is determined.

[0028]

[0028] is the controller 180 is configured to largely include an image authentication processing unit 10, a voice authentication processing unit 40, statistical model management unit 50, and the authentication judgment section 290. The controller 180 may control the overall operation of the operational features of the present invention, the operation example of the user device 100 with reference to the drawings described below for the detailed control operation of the controller 180 and in its control method it will be described.

[0029]

[0029] Meanwhile, the controller 180 may control the various operations associated with the conventional functions of the user device 100. In addition to the functions of the present invention. For example, the controller 180 may in response to a touch event that is input via the input interface of the touch-based, control the operating features thereof. In addition, the controller 180 may be a wired based or wireless communication based on communication control transmission and reception of various data. And the controller 180 CPU (Central Processing Unit), GPU (Graphical Processing Unit), and memory, such as a single chip (chip) in the built-in the system-on-chip (SoC, System on Chip) implementation will be there. Each configuration of the SoC is connected to the system bus (system bus) data communication can be made between them. Or the control section 180 may be CPU, GPU, and a memory and the like, packaged (packaging) into a multi-layer (multi layer).

[0030]

[0030] User and device of the present invention shown in FIG. 1 100 may include all information communication devices, multimedia devices, and application devices thereof has a structure for supporting the user authentication techniques of the present invention. For example, the user device 100 has various communication systems in response to which each communication protocols (communication protocols) in accordance with operation of the mobile communication terminal for, including, tablet PC (Personal Computer), a smart phone (Smart Phone), a digital camera, PMP (portable Multimedia player), media player (media player), a mobile game terminal and PDA (Personal digital Assistant), etc. can be included in the device has. In addition, the method of the present invention is applied to various devices, such as digital TV (Digital Television), DS (Digital Signage), LFD (Large Format Display), a laptop computer may be operated.

[0031]

[0031] FIG. 2 is a diagram schematically showing the configuration of the controller 180 according to an embodiment of the present invention.

[0032]

[0032] Referring to FIG. 2, the invention of the control section 180 is image authentication processing section (10 to process the facial feature vector, and the user authentication by the object feature vector detected from the image obtained through the camera module 110), delivered from the voice authentication processing unit 40, and the image authentication processing unit 10 and the voice authentication processing unit 40 to process the user authentication by the speech feature vector detected from the voice acquired through the microphone 123 is configured to include a plurality of authentication information (e.g., face authentication information, authentication information, and voice) based on the authentication judgment section 290 for processing integrated authentication for the user. And particular with the image authentication processing unit 10 face authentication processing unit 20 for processing the face authentication by the static feature vector is detected based on the captured (capture) the still image from the acquired image, based on the acquired image is configured to include an authentication processing unit for processing an object object the object authenticated by the detection of the dynamic feature vector (for example, face, eyes, lips, etc.) (30). That distinguishes the particular area of the face in the object image is recognized in the present invention, it may comprise a self-face, eyes, lips and so on as before. And the object to be detected from the object feature vector may be a dynamic feature vectors, such as the movement of the face, eye blinks, the movement of lips is detected.

[0033]

[0033] The above face authentication processing section 20 is configured to include a face extraction unit 210, a first feature vector detection unit 220, and the face authentication unit 230.

[0034]

[0034] to the face extraction unit 210 extracts a user's face from the image input through the camera module 110. For example, the face extraction unit 210 and outputs the extracted features, such as facial areas, eye areas, and mouth area from an input facial image. The face detection unit 210 in the present invention, is inputted from the camera module 110, the display unit and captures an image displayed through the 130, with the captured still image to perform the user's face recognition and facial feature extraction can.

[0035]

[0035] The first feature vector detection unit 220 is the distance and angle are generated to take a point between the facial feature vector (for example, face eyes, nose, and mouth from the features extracted by the face extraction unit 210, and color the like) can be detected. For example, the first feature vector detection unit 220 by using a center point of the eye of the features extracted in the face extraction unit 210, and performs normalization for the face shape, a specific face in the normalized face image and outputs the extracted facial feature vector.

[0036]

[0036] comparing the face authentication unit 230 is the first feature vector detection unit 220, the pre-register the unique features of the facial feature vector face information of the face extracted from the (in particular, the face recognition statistical models) by performing an authentication of the face image, and outputs the authentication information according to the authentication result. For example, the face authentication unit 230 compares the extracted facial feature vector is pre-learned and stored in the face information, and can be determined for a match between them. In this case, the determination whether the match may be determined in consideration of the error range is set, for example, may output the authentication information indicating that the authenticated user to match at least 90%. On the other hand, can output the authentication information indicating that the unauthorized user when (even if that means that no face is taken if there are no facial feature vector) matches less than 90%. Based on the probability value for determining whether or not the matching may be set variously, such as 80%, 85%, depending on the user settings, including the 90%.

[0037]

[0037] The object authentication processing unit 30 is configured to include an object detection unit 240, a second feature vector estimation unit 250, and the operation determination unit 260. The object authentication processing unit 30 in the present invention, images input from the camera module 110 (in particular, video) through the object (for example, face, eyes, mouth, etc.) for detecting the operation to determine whether the object movement it may correspond to a recognizer.

[0038]

[0038] The object detection unit 240 extracts the object from the image input through the camera module 110. The object in this invention is a factor to determine the movement from the user's face, or the like may be the face, eyes, mouth. For example, the object detection unit 240 may output the extracted face region, eyes area, and the area of the mouth region of the object set from an input facial image. In other words, the object detection unit 240 is input from the camera module 110 can detect the position of the object is set in the image being displayed through the display unit 130.

[0039]

[0039] The second feature vector detection unit 250, the object feature vector showing the operation (movement) of the object from the detected position of the object in the object detection unit 240 (for example, the movement of the face, blinking of the eyes, mouth the can detect the movement, etc.). For example, the second feature vector estimation unit 250 extracts the feature vectors based on the size, the shape of the lips such as lip which is changed according to the movement of the mouth of the features extracted from the object detection unit 240 outputs can do. Or the second feature vector detecting section 250 can output the extracted feature vector of the eye features extracted from the object detection unit 240 is to be changed

(corresponding to the blinking of the eye). Or the second feature vector detecting section 250 can output the extracted feature vector, such as change in size of the face according to the movement of the face of the features extracted from the object detection unit 240, the position of the face changes.

[0040]

[0040] in the operation determination unit 260 and performs authentication for the user to determine whether the operation (movement) of the object from the object feature vector detected in the second feature vector estimation unit 250, the authentication result outputs in accordance with operation information (authentication information). For example, the operation determination unit 250 may output the operation information indicating that the operation when determining that the movement of the object. On the other hand, the operation determination unit 250 may output the operation information indicating that no operation when determining that there is no movement of the object.

[0041]

[0041] The voice authentication is processing section 40 is configured to include a third feature vector detection unit 270 and the voice authentication unit 280.

[0042]

[0042] detecting the third feature vector detecting section 270 is the speech feature vectors from the voice input through the microphone 123 (e.g., tone (tone), the frequency (frequency), vocabulary, speed, etc.) to be output can. In this case, the third feature vector detecting section 270 may detect at least one feature vector in accordance with the operation method of the authentication voice. For instance, voice way authentication operation method for that operation, regardless of the vocabulary user speaking when the (e. G., The user speaks the words and is independent of the authentication method to separate only the tone or frequency), wherein the third feature vector detector 270 may detect at least one feature vector set of feature vectors of the tone, frequency, speed and the like of the voice. Or way operation method for voice authentication is operated to separate the vocabulary user speaking when the (e. G., Authentication method that requires the input preset word), the third feature vector detecting section 270 is tone of voice, frequency, it can be detected with the at least one feature vector and the feature vector of the speech vocabulary that are separated from the set of the characteristics of the speed vector.

[0043]

[0043] compared to the voice authentication unit 280 has the third feature vector detection unit 270, the voice of the unique characteristics of the speech feature vector previously registered voice information (in particular, the statistical models for speech recognition) detected in by performing an authentication of the voice, and outputs the authentication information according to the authentication result. For example, the voice authentication unit 280 compares the pre-study and the detected speech feature vector stored in the voice information, it is possible to determine whether a match between them. In this case, the determination whether the match may be determined in consideration of the error range is set, for example, may output the authentication information indicating that the authenticated user to match at least 90%. On the other hand, can output the authentication information indicating that the unauthorized user when (even if that means that the voice is input when there is no speech feature vector) matches less than 90%. Based on the probability values for a match for the determination may be set variously, such as 80%, 85%, depending on the user settings, including the 90%.

[0044]

[0044] Further, the voice authentication unit 280 may perform the authentication using the at least one feature vector in accordance with the operation method of the authentication voice. For example, the operation method for voice authentication if the way the operation, regardless of the vocabulary you speak, the voice authentication unit 280 in advance and the feature vector that is passed is detected by the third feature vector estimation unit 270 the learning of the audio information can be

performed by comparing only the features his authentication vector corresponding to the feature vector. On the other hand, if the operation method for voice authentication manner that operate to separate the vocabulary you speak, the voice authentication unit 280 has the third feature vector detection unit 270, feature vectors of the lexical feature vector that is passed from the audio information pre-study (in particular, lexical feature vector) by comparing the authentication may be (for example, that the input word is determined and the learning word matches). That is, the voice authentication unit 280 may perform authentication for the vocabulary of the speech input as compared to the recognized vocabulary training feature vector lexical feature vector. And wherein the voice authentication unit 280 has a different feature vectors (e.g., tone, frequency, at least one of the speed), pre-study and that is when it passes the authentication for the lexical feature vectors transmitted from the third feature vector estimation unit 270 the audio information may be carried in his authentication by comparing the (at least one in particular, tone, frequency, speed). The voice authentication method can be variously set according to a user operation.

[0045]

[0045] Speech is transmitted from the authentication determination unit 290 is the face authentication processing section 20, face authentication information, motion information, and the voice authentication processing unit 40 is passed in the object authentication processing unit 30, which is passed from the by using the authentication information may be an integrated authentication, and outputs an authentication result thereof. The authentication determination unit 290 is the user authentication can be processed during normal indicate that passed the face authentication information, motion information, and by analyzing both the audio user authentication credentials. Or the authentication determination unit 290 analyzes the face authentication information, operation information, and the authentication voice communication any one error can handle the user authentication indicating that the unauthorized user. For example, the authentication judgment section 290 is to confirm that the authenticated user's face through a face authentication information and, upon confirmation that the user voice authentication through voice authentication information, and determine an operating state of the object determined by the operation information the user authentication can be processed successfully. On the other hand, the authentication judgment section 290 is confirmed that unauthorized users face through the face authentication information, or when confirmation that a non-authenticated user's voice through a voice authentication information, or determine the non-operating state of a determined object or through the operation information it may be a user authentication error process.

[0046]

[0046] Figure 3 is a diagram schematically showing a configuration of a controller 180 according to an embodiment of the present invention.

[0047]

[0047] Referring to FIG 3, the controller 180 of the present invention, image authentication processing unit 10 to process the user authentication by the face feature vector detected from the image obtained through the camera module 110, the microphone voice authentication processing unit 40, and the image authentication processing unit 10 and each of the authentication information sent from the voice authentication processing unit 40 to process the user authentication by the speech feature vector detected from the voice acquired through 123 s is configured to include an authentication judgment unit 290, based on the (e.g., face authentication information, authentication information, voice, etc.) for processing integrated authentication for the user. And the image authentication processing unit 10 is a specific object (for example, the face authentication processing unit 20 for processing the face authentication by the static feature vector is detected based on the captured still image from the acquired image, based on the acquired image , it is configured to include an object authentication processing unit 30 to process the authentication object according to the dynamic feature vector detected in the face, eye, lips, etc.).

[0048]

[0048] As shown in FIG 3, the configuration of the controller 180 according to another embodiment of the invention may take the configuration of the operation determination unit 260 of the configuration of the reference to Figure 2 the controller 180 is omitted and it includes the synchronization judgment unit 300, and thus can vary to the integrated authentication method of the authentication determination unit 290. And thus the reference numbers which are the same in configuration matching the description of the previously referenced FIG. 2, overlapping descriptions will be omitted. And the present invention, eoteuna represented by separating the configuration and the configuration of the controller of Figure 3 (180) of the control unit 2 (180), operation of the operation determination unit and the synchronization judgment unit 300 and the operation of the 260 the operation can be combined into a single configuration or may, in the controller 180 can be the two configurations are all configured, of course. Or less, and the difference of the configuration of Figure 3 the control unit 180, the controller 180 of Figure 2 in the configuration of the part will be described.

[0049]

[0049] The second feature vector detection unit 250, the object feature vector showing the operation (movement) of the object from the detected position of the object in the object detection unit 240 (e.g., a face of said object authentication processing unit 30 detecting a motion, such as flickering, movement of the mouth of the eye) and can be output. In particular, FIG. 3 shows the case where the object is ipin, and thus detects the object feature vector in accordance with the size changes, shape changes in the lip of the lips according to the movement of the mouth to illustrate that the output to the synchronization judgment unit 300 It will be described.

[0050]

[0050] Further, the third feature vector estimation unit 270 is speech feature vector (e.g., tone, frequency, vocabulary, speed from the voice inputted through the microphone 123, as described previously in the voice authentication processing unit 40 detect, etc.) and can be output. In this case, the third feature vector detecting section 270 can be respectively output the detected speech feature vector to the synchronization judgment unit 300, including the voice authentication unit 280.

[0051]

[0051] On the other hand, the synchronization judgment unit 300 by using a speech feature vector that is passed in the object feature vector that is passed from the second feature vector 250 and the third feature vector 270, the two feature vectors determine whether they are synchronized in time, and outputs the synchronization information over. For example, the synchronization judgment unit 300 may determine whether the comparison of the speech dynamics in accordance with the audio object and the lips motion according to the moving object and a feature vector, both attributes are synchronized. Here, the way through the synchronization judgment is already trained statistical model (for example, statistical models learn the lip motion and voice) lip objects has a dynamic feature vectors, determines whether the speech feature vector is detected correspondingly It may be made. Or the synchronization judgment is the starting point of the utterance to detect the start and end points of the real speech act that is, ignition (utterance) to the end of taking a sound based on the characteristic vector of the lips object without the statistical model, based on the speech feature vector and detecting an end point, it can be made by comparing the two detected values.

[0052]

[0052] Speech is transmitted from the authentication determination unit 290 is the face authentication processing section 20, face authentication information, the synchronization judgment unit 300, synchronization information, and the voice authentication processing unit 40, which is passed from being passed in by using the authentication information may be an integrated authentication, and outputs an authentication result thereof. The authentication determination unit 290 is passed to the face authentication information, it is possible to process the normal user authentication indicate that synchronization information, and analyzes the voice authentication information both authenticated users. Or the authentication determination unit 290 analyzes the face authentication information, synchronization information, and voice authentication information forwarding

any one may be a user authentication error process to indicate that a non-authenticated user. For example, among the authentication determination unit 290 is to confirm that the authenticated user's face through a face authentication information, voice authentication information object feature vector, and to confirm that the authenticated user voice, through the synchronization information through a speech feature vector It may process a normal user authentication to confirm that the sync is matched. On the other hand, synchronization between the authentication judgment section 290 is face to confirm that the authentication information unauthorized users face through or voice via the authentication information to confirm that unauthorized user speech, or object feature vector with the speech feature from the synchronization information vector the error process can confirm that the user authentication does not match.

[0053]

[0053] Figure 4 is a schematic diagram illustrating a configuration of the statistical model management unit 50 in the controller 180 according to an embodiment of the present invention.

[0054]

[0054] Referring to Figure 4, the statistical model management unit 50 of the present invention is configured to include the face authentication learning unit 410, learning voice authentication unit 420, and learning information processor (430).

[0055]

[0055] The face authentication learning unit 410 and outputs the authentication processing based on the image feature vector of the face to be processed through a 10, as previously discussed to generate a statistical model for face recognition.

[0056]

[0056] The voice authentication learning unit 420 may be output to generate a statistical model for the speech recognition based on the voice authentication processing of speech feature vector to be processed through a 40, as previously discussed.

[0057]

[0057] The facial feature vector, the object feature vectors, and speech feature for user authentication for a vector, a statistical model for the face recognition and the speech recognition statistical model for which the learning information processing unit 430 is detected in the authentication mode, it can be stored in the storage unit 140. The learning information processor 430 may be stored in each storage area is assigned to the repeated learning based on the statistical model for face recognition and voice recognition statistical model for the face information and audio information. At this time, if information of the face and separated by a feature vector and the feature vector of an object faces based on statistical models for the trained face detection can be managed. And separated by a feature vector as the audio if the information words for the same unique as tone, frequency, speed of the speech based on statistical models for the trained speech recognition feature vectors and security certificates (for example, such words corresponding to the password) It may be managed.

[0058]

[0058] Figure 5 is a diagram illustrating an exemplary operation for authenticating the user by using the composite biometric information from the user device 100 in accordance with an embodiment of the present invention.

[0059]

[0059] illustrates an example of the case where the mode is to be activated in order to release the lock of the screen, particularly, in the Figure 5 the user device 100.

[0060]

[0060] Referring to FIG 5, reference numerals <501> the user device 100, as shown in the display section 130 is turned on in accordance with the waiting mode in the off (turn-off) condition, a user's operation (display section 130 of turn-on (turn-on) for enabling a user of a hot key (hot key) input actions, etc.) to by reference number <503> in the illustrated described as display unit 130 is turned on to be able there. in this case, it is assumed that the Fig. 5, the user of the lock and the lock setting screen, is set for it in order to protect the user device 100. Therefore, the display unit 130 is turned on, the turn on-off state when switched to an on state, the controller 180 represent a lock screen set by the user as shown in the reference number <503> in the display section 130 can.

[0061]

[0061] Next, the control unit 180 may determine whether the reference number <503> for the user and the authentication mode of the authentication screen is set as to provide a lock. Then, the controller 180 may drive the authentication mode is set when the camera module 110 and the microphone 123, and to execute the authentication mode.

[0062]

[0062] Next, the controller 180 is an image obtained through the camera module 110 as shown in reference number <505> can be represented on the display unit 130. For example, the user the display unit 130 turned on can be located on the user device 100 area to be photographed the user's face over the whole when the camera module 110 (in particular, the front camera). Then, the controller 180 may display an image by passing him (in particular, the user face image) to be input through the camera module 110 to a display 130. At this time, the controller 180 is an image input through the camera module 110 to an area of the lock shown in the screen display 130 can indicate to the overlay (overlay). Or controller 180 may display screen lock omitted, and only indicate the images input through the camera module 110.

[0063]

[0063] Next, a user may ignite the voice When the face of the user through the display section 130 as shown in the reference number <505>. Then, the display section 130, the reference number <505> to Reference <509> may appear in the image is changed according to the user's utterance, as shown. At this time, the controller 180 features for user authentication from the video image and display an image input through the camera module 110 through the display 130, the input vector (for example, the facial feature vector, and the object feature vector) It can be detected. In addition, the controller 180 may detect the feature vectors (e. G., Tone of voice, frequency, words, sounds and so on) for user authentication from the voice inputted through the microphone 123.

[0064]

[0064] Next, the controller 180 voice authentication using the speech feature vector detected from the input speech of the face authentication, the microphone 123 with the facial feature vector detected from the input image of the camera module 110, and it may perform the authentication objects using the object feature vector detected in the input image. Then, the controller 180 may perform the final authentication for the user to collect all of the results according to the face authentication, voice authentication, and the authentication object. For example, the controller 180 and ensure that the authenticated user's face through the face authentication, and confirm that the user voice authentication via the voice authentication, comprising the operations of the object through the object authentication (e.g., face of movement, when check the blinking of the eye, such as the motion of the mouth) it can be determined to be an authenticated user to the user.

[0065]

[0065] or the controller 180 voice authentication using the speech feature vector detected from the input speech of the face authentication, the microphone 123 with the facial feature vector detected from the input image of the camera module 110, and the feature vector of the detected object from the input image and can perform the lip motion and synchronization between the authentication voice based on the speech feature vector. Then, the controller 180 may perform the final authentication for the user to collect all of the results according to the face authentication, voice authentication, and authentication synchronization. For example, the controller 180 matches the check that the authenticated user's face through the face authentication, and confirm that the user voice authentication via the voice authentication, and lips operation in voice ignited via the synchronization authentication and subsequent you can see that when it is determined that the user is authenticated users.

[0066]

[0066] Next, the controller 180 can normally handle the user authentication to determine that the user is authenticated by the user authentication, such as the complex and release the authentication mode. For example, the controller 180 may control the execution screen displayed as shown in the locked and released, and the reference number <511> ellipses of the lock screen. May represent a - (display turned off state entry), such as an application execution screen of a previously executed in the execution screen is the home screen, or the user device 100 is in standby mode.

[0067]

Thus [0067], according to the embodiment of the present invention, further performs user authentication using the composite biometric information, adding the operation state of the object feature vectors detected, adding sensing the synchronization state of the lips motion and the input speech enhanced than by the user authentication can be performed. Accordingly, to prevent the illegal use of the user device the user and the licensee of the pictures and the user device 100 as a recording audio to be illegal use 100, or the user authentication is to block the advance access to a wealth of information required can. And more than that described in the authentication mode of the present invention is applied to an example for releasing the lock of the lock screen. However, the authentication mode according to the embodiment of the present invention, information that you want to protect from other users (e.g., address book, personal data, etc.), the user device determines whether or not (100) allows a financial service access using, and the user device (set the authentication mode for the charging or the like occurs in the service 100), and may perform the user authentication, such as integrated earlier.

[0068]

[0068] Figure 6 is a flow chart showing the statistical model registration method for user authentication, the user device 100 according to an embodiment of the present invention.

[0069]

[0069] Referring to FIG 6, the controller 180 may drive the certification authentication configuration setting mode entry (step 601) in response to a user request (step 603). The authentication-related configuration denotes a configuration for a complex recognition biometric information, the present invention may include a camera module 110 and a microphone 123. Here, the Fig. 6 but omitted, in which you can select the category (category) to be set to perform the authentication mode, and enters the authentication mode, the user interface can be provided (UI, User Interface). For example, you can set the authentication mode for the various categories, such as lock release function is executed when the authentication mode, authentication mode when running the Address Book entry, financial services, certification Run mode entry, billing services authentication mode when running entry. And upon completion of setting the one or more categories through the user interface may be implemented so that the driving certification configuration.

[0070]

[0070] Next, the controller 180 the authentication-related configuration (especially, the camera module 110 and the microphone 123) when the drive, and acquires a face image that is passed through the camera module 110 (605 step) it may obtain a voice transferred through the microphone 123 (step 607). That is, the statistical model for the user authentication in the present invention can be composed to face the learning process and is divided into speech learning process, the face learning process and the voice learning statistical models for face recognition through voice recognition statistical model for have. At this time, the face and the voice learning process learning process can take place simultaneously or individually progress (time series), according to FIG. 6 shows as an example a processing operation which is simultaneously in parallel. The parallel or series operation method of each of the learning process can be determined according to user setting.

[0071]

[0071] According to the face learning process, the controller 180 may detect the facial feature vector extracted from the acquired face and the face (step 611) from the image, the extracted face (step 613). For example, the controller 180 is to distinguish the features of the face such as the face area from the image input through the camera module 110, the eye region, and the mouth area to extract the face. Then, the controller 180 may detect a facial feature vector from the normalized face image, perform the normalization, and for the face shape by using a center point of the eye of the characteristics of the extracted face. Next, the controller 180 is the area (for example, face information storage area of the facial feature vector using via the face authentication learning (step 615) to generate a statistical model for face detection (step 617), storage unit 140 can be stored in 160) (step 619). For example, the controller 180 SVM (Support Vector Machine), such as a machine learning algorithm (machine learning algorithm) based in the facial feature vector to for learning performed by a user face authenticating for determining based on the face recognition for statistics It can build the model.

[0072]

[0072] According to the speech learning process, the controller 180 can detect the speech feature vector from the acquired voice (step 621). For example, the controller 180 analyzes the characteristics of the tone, frequency, vocabulary, and speed from the voice inputted through the microphone 123 can detect the speech feature vector. Then, the controller 180 is the area (for example, of generating a statistical model for a speech recognition through voice authentication learning (step 623) (step 625), a storage unit 140, using the speech feature vector, the audio information storage area (170 there)) to be stored (step 627). For example, controller 180 may be based on a machine learning algorithm such as SVM as before performing the learning for the speech feature vector to establish a determination based on the voice recognition statistical models for the user voice authentication.

[0073]

[0073] On the other hand, the Fig. 6 but omitted, the user can make further settings for the operation method of the authentication mode. For example, the authentication face as described with reference to FIG before, voice authentication, and the integrated authentication method that is based on the object motion change authentication, authentication face as described with reference to the above Figure 3, voice authentication, and synchronization authentication (lips object variation of the operating and integrated authentication method that is based on whether the synchronization between the input speech) can be set to any one of the methods. At this time, it may be set in addition to the object type (for example, the movement of the face, such as flickering, movement of the mouth of the eye) to be certified if the change operation of the electronic architecture of the authentication method.

[0074]

Figure [0074] 7 is a flow chart illustrating a user authentication method from the user device 100 according to an embodiment of the present invention.

[0075]

[0075] Referring to FIG. 7, the control unit 180 may execute in response to certain features of the user device 100 to drive the authentication-related configuration authentication mode entry (step 701) (step 703). For example, the controller 180 may determine whether the user is at the specific function execution request, the authentication mode for the user authentication is set in the function execution. If the authentication mode is set in the function execution can be controlled enters the authentication mode. Then, the controller 180 may drive the camera module 110 and the microphone 123 is set for user authentication when the authentication mode entry. The features that set the authentication mode may be based on user settings, such as, locked, financial services, billing services, and contacts as previously discussed.

[0076]

[0076] Next, the controller 180 when the drive is the authentication-related configuration, obtain a facial image, and (step 705) is passed through the camera module 110 obtains a voice transferred through the microphone 123 it can be (step 707). The authentication process for the user authentication in the present invention is largely divided into a video and a voice authentication process, the authentication process, the authentication image and the voice verification process may be operated in parallel or in time series. And the image authentication process can be largely divided into the face authentication process and the object authentication, face authentication, and the authentication process object may be operated in parallel or in time series. The parallel or series operation method of each of the authentication process can be determined by the user settings.

[0077]

[0077] According to a face authentication process of the image authentication process, the controller 180 extracts the face from the acquired face image, and (step 711), it is possible to detect the facial feature vector (step 713) from the extracted face . For example, the controller 180 is to distinguish the features of the face such as the face area from the image input through the camera module 110, the eye region, and the mouth area to extract the face. Then, the controller 180 may detect a facial feature vector from the normalized face image, perform the normalization, and for the face shape by using a center point of the eye of the characteristics of the extracted face. Next, the controller 180 is the facial feature vector and the learning by comparing the face recognition statistical model for performing face authentication, and (step 715), may generate a face authentication information accordingly (step 717).

[0078]

[0078] According to the object the authentication process of the image authentication process, the controller 180 defects the object from the obtained face image, and (step 721), it is possible to detect the object feature vector from the detected object (723 steps) . The object is to determine the elements to move from the user's face, in the Figure 7 may correspond on the face, eyes, mouth. For example, the controller 180 the operation of the object from the detected position of the face region, the eye area, and the location of the object set of the mouth area from the face image input through the camera module 110, and detects the object the (moving) object feature vectors representing the (e. g., the movement of the face, such as blinking, eye movement of the mouth) can be detected. Next, the controller 180 may generate the operation information in accordance with operation, and determines whether or not (step 725) of the object from the object feature vectors, thereto (step 725).

[0079]

[0079] According to the voice authentication process, the controller 180 can detect the speech feature vector from the acquired voice (step 731). For example, the controller 180 from the voice inputted through the microphone 123, analyzes the characteristics of the tone, frequency, vocabulary, speed and the like can detect the speech feature vector. Then, the controller 180 may generate the speech feature vector to perform voice verification by comparing the statistical model for the speech recognition and learning (step 733), the voice authentication information accordingly (step 735).

[0080]

[0080] Next, the controller 180 is the face authentication information, motion information, and an integrated authentication based on a voice authentication information (741 steps), and outputs an authentication result according thereto (743 steps). For example, the controller 180 upon check the operation of the object and confirm that the authenticated user's face via the face authentication information, and to confirm that the user voice authentication via the voice authentication information, via the operating information yirueojim the handle user authentication for the normal user, and outputs an authentication result according thereto may be (for example, the lock release screen, allowing the billing service, the address book lights). Or controller 180 during check to confirm that unauthorized user's face via the face authentication information, or to confirm that the voice credential unauthorized user speech via, or not be in a motion of the object through the operation information the error processing for the user authentication of the user, and outputs an authentication result accordingly (error feedback information output corresponding to the authentication failure, etc.) can be.

[0081]

Figure [0081] 8 is a flow chart illustrating a user authentication method from the user device 100 according to an embodiment of the present invention.

[0082]

[0082] Referring to Figure 8, the controller 180 previously described user device specific features camera module 110 and the microphone 123, the authentication mode entry in response to the execution (step 801) of 100 as described with it can drive the same certification configuration (step 803).

[0083]

[0083] Next, the controller 180 when the drive is the authentication-related configuration, obtain a facial image, and (step 805) is passed through the camera module 110 obtains a voice transferred through the microphone 123 it can be (step 807). The authentication process for the user authentication in the present invention significantly is divided into image authentication and voice authentication process, as previously discussed, and the image authentication process can be largely divided into the face authentication process and the object authentication process, this authentication process are according to the operational method can be accomplished in parallel or in time series.

[0084]

[0084] According to a face authentication process of the image authentication process, the controller 180 extracts the face from the acquired face image, and (step 811), it is possible to detect the facial feature vector (step 813) from the extracted face . And the controller 180 performs face authentication of the user by comparing for learning and the detected facial feature vector facial recognition statistical model (step 815), may generate a face authentication information accordingly (817 steps).

[0085]

[0085] According to the object the authentication process of the image authentication process, the controller 180 detects the object from the obtained face image, and (step 821), it is possible to detect the object feature vector from the detected object (step 823) . Then, the controller 180 is based on the object feature vector with the speech feature vector detected in the voice authentication process, checks every sync between the two feature vectors (step 825), may generate the synchronization information over (step 827). That is, the controller 180 may determine whether the object feature vectors with the speech feature vector is synchronized in time. For example, the controller 180 may determine whether or not the compared voice dynamic characteristics of the object according to the voice and the lips motion according to the moving object and a feature vector, both attributes are synchronized. Then, the controller 180 may generate the synchronization information according to the determination whether the sync.

[0086]

[0086] According to the voice authentication process, the controller 180 can detect the speech feature vector from the acquired voice (step 831). And the controller 180 performs voice authentication of the user by comparing the learning for the speech feature vector to the detected speech recognition models and statistics (step 833), may generate a voice authentication information thereof. The controller 180 may perform voice and the authentication using the detected speech feature vector, as described above, performs the synchronization between the authentication voice feature vector and the feature vector objects.

[0087]

[0087] Next, the controller 180 is the face authentication information, synchronization information, and an integrated authentication based on a voice authentication information (step 841), and outputs an authentication result according thereto (843 steps). For example, the controller 180 between the check that the face authentication of the user's face through the authentication information, and the audio through the authentication information to confirm that the authenticated user's voice, and an object feature vector over the sync information and the speech feature vector synchronization is successful, the authentication of the user when the check for a match, and may output an authentication result thereof. Or controller 180 determine that the user faces the non-authenticated via the face authentication information, or via the voice authentication information to confirm that unauthorized user's voice, or via the synchronization information is synchronized between the object feature vector with the speech feature vector when the check does not match the error processing the user authentication for the user and may output an authentication result thereof.

[0088]

[0088] Figure 9 is a flowchart illustrating an operating method for user authentication, the user device 100 according to an embodiment of the present invention.

[0089]

[0089] In particular, FIG. 9, is provided of the camera module 110 and the microphone 123 days biometric information from any one, if they are not provided by the other biometric information from the other, whether an error or validity thereof a illustrates the operation of determining.

[0090]

[0090] Referring to FIG 9, the controller 180 has previously described the user device-specific function camera module 110 and the microphone 123, the authentication mode entry in response to the execution (step 901) of 100 as described with it can drive the same certification configuration (step 903).

[0091]

[0091] controller 180 when the authentication-related configuration is driving, from the camera module 110 and the microphone 123 may determine whether at least one of biometric information is detected (step 905).

[0092]

[0092] controller 180 (NO in step 905) is determined, and (919 steps) as a user authentication error when it can not detect any biometric information from the camera module 110 and a microphone 123, an error feedback corresponding It may control the information output (step 921). This is, without the user's face is input through the camera module 110, the user's voice may be a non-input state through the microphone 123. In this case, although the not shown in Figure 9, the controller 180 may decide to then wait for the biometric information detected during a preset time when the error is determined, an error when the set time has elapsed until the biometric information is not detected have.

[0093]

[0093] The controller 180 is a composite biometric to at least one of the biometric information of the detected biometric information (YES in step 905), upon being detected by the camera module 110 and the microphone 123 correspond to the pluralily may determine that the information (step 907). Then, the controller 180 may perform the authentication using the composite integrated biometric information in accordance with the procedures as discussed previously (YES in step 907) to determine when the compound to be the biometric information (step 909). On the other hand, the controller 180 may determine that the image recognition information to be determined when one of the biometric information (NO in step 907) wherein the biometric information that corresponds to the recognized voice information (step 911).

[0094]

[0094] The controller 180 is a voice authentication in accordance with the procedures as discussed earlier by using the voice input through the 911 speech recognition information of the microphone (123) when (in step 911 YES), be determined at step while performing, for image capture by the camera module 110 may wait (step 913). The control unit 180 may check whether the image capture in the air image capture (step 915).

[0095]

[0095] The controller 180 may perform when the integrated image is obtained on (YES in step 915), the user authentication (step 909). At this time, the control unit 180 is integrated authentication as after performing image authentication using the picture input through the camera module 1110, based on the image authentication information according to a voice authentication information and the image authentication in accordance with the voice authentication it can be carried.

[0096]

[0096] The controller 180 may determine if the image is not obtained unless (NO in step 915), speech input through the microphone 123 is terminated (step 917). The controller 180 may perform the following operation proceeds to the step 913. If the voice input is not terminated (NO in step 917). Controller 180 when the voice input is terminated (YES in step 917) and determines a user authentication error (step 919), it is possible to control the output error feedback information accordingly (step 921).

[0097]

[0097] The controller 180 includes an image authentication in accordance with the procedures as discussed earlier by using the image input through the 911 image recognition information as being (NO in step 911), the camera module to be determined (110) in step while performing, it may wait for a voice obtained by the microphone 123 (step 923). The control unit 180 may check whether a voice acquiring voice in the air obtained (step 925).

[0098]

[0098] The controller 180 may perform authentication for the integration (YES in step 925), if the user voice is acquired (step 929). At this time, the controller 180 is an integrated authentication as after performing the voice authentication using the input voice through the microphone (123), based on the voice authentication information in response to the video authentication information and the voice authentication in accordance with the image authentication it can be carried out.

[0099]

[0099] The controller 180 may determine whether if the voice is not acquired (NO in step 925), the set time predefined elapsed (step 927). The controller 180 may If the set time has not elapsed (NO in step 927) to perform the following operation proceeds

to the step 923. Controller 180 when the set time has elapsed (YES in step 927) and determines a user authentication error (step 919), it is possible to control the output error feedback information accordingly (step 921).

[0100]

[0100] On the other hand, the user can act to position a number of reasons the microphone 123 when the ignition for the user when the user authentication using the user device 100, voice authentication around the users mouth. For example, in the situation that must be ignited at a quiet voice or prevent leakage of the quiet environment of utterance from the others, a user may ignite the microphone 123 adjacent to the users mouth. In such a case, by the camera module 110 may be a user's face is not recognized state. Or the user after recognizing the user's face may be left first input time difference to the ignition for voice input. Thus, considering a variety of environments, such as above in the present invention, each of the biometric information by any of the biometric information only enter a range of biometric information even when the recognition, are not recognized in accordance with the set routine is not recognized at the same time through to the atmosphere to reduce the error determination made reckless user intention and is irrespective.

[0101]

[0101] On the other hand, the user authentication method using a composite biometric information from the user device of the present invention as described above is implemented in program instruction form that can be executed by various computer means to be recorded on a computer-readable recording medium have. At this time, the computer-readable recording media may also include, alone or in combination with the program instructions, data files, data structures, and the like. Meanwhile, the program command recorded on the recording medium may be the kind well known and available to those skilled in the art of computer-designed and configured specially for the present invention.

[0102]

[0102] The computer-readable media include hard disks, floppy disks, and magnetic tape, such as magnetic media (Magnetic Media), CD-ROM (Compact Disc Read Only Memory), DVD (Digital Versatile Disc) and the like optical recording medium (optical media), flop tikeol disk (Floptical disk), such as magneto-optical media (Magneto-optical media), and ROM (Read Only memory), RAM (Random Access memory), flash memory, etc., such as program instructions to store and perform hardware devices that are specially configured to. In addition, the program command containing higher level code that may be both machine code, such as produced by a compiler, and executed by the computer using an interpreter. The above-described hardware devices may be configured to act as one or more software modules in order to perform the operations of the present invention, or vice versa.

[0103]

[0103] And embodiments of the invention disclosed in the specification and drawings are merely be presented specific examples to aid the understanding of the present and easily describe the technical details of the present invention invention and are not intended to limit the scope of the invention . Therefore, the scope of the invention in addition to the embodiments disclosed herein should be construed to be any change or variation which is derived on the basis of the technical idea of the present invention within the scope of the invention.

[0104] 100: the user device 110: the camera module 120: an audio processor 121: speaker 123: Mike 130: display unit 140: a storage unit 150: learning information storage 160: face information storage 170: the voice data storage area 180: the control unit 10 : image authentication processing 40: 50 voice authentication process: statistical model management 260: operation judging section 290: authentication judgment section 300: synchronization judgment unit

Patent Translate
Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

CLAIMS KR20130097581

1.

One. In the user authentication method, comprising the steps of: obtaining a plurality of different biometric information for the user authentication; generating the respective authentication information for a plurality of biometric information obtained; based on the authentication information generated integrated user the user authentication method comprising a procedure of authentication.

2.

2. According to claim 1, wherein the step of the acquisition process for acquiring image information through a camera module; user authentication method comprising the step of obtaining audio information through the microphone.

3.

3. The authentication using the face feature vector; according to claim 2, wherein the step of the generation process for detecting a speech feature vector by detecting a facial feature vector, and the object feature vector based on the image information, and based on the voice information for generating a face authentication information; generating a voice authentication information for the authentication with the speech feature vector; user authentication comprises the step of generating the motion information for the authentication by using the object feature vectors Way.

4.

4. According to claim 3, wherein the operation information, the user authentication method, characterized in that the information indicating the operating state of the set object.

5.

5. According to claim 3, wherein the step of performing the user authentication method comprising the step of determining whether the last authentication, based on the face authentication information, the voice authentication information, and the operation information.

6.

6. The method of claim 5, wherein the face authentication information, the voice authentication information and user authentication method characterized in that at least one of the operation information further includes the step of determining when an error is not normal authentication.

7.

7. The authentication using the face feature vector; according to claim 2, wherein the step of the generation process for detecting a speech feature vector by detecting a facial feature vector, and the object feature vector based on the image information, and based on the voice information for generating a face authentication information; generating a voice authentication information for the authentication with the speech feature vector; in that it comprises the step of generating the synchronization information for the authentication by using the object feature vector with the speech feature vector user authentication method according to claim.

8.

8. The method of claim 7, wherein the synchronization information is the user authentication method, characterized in that the information indicating that the object feature vectors with the speech feature vectors are synchronized in time.

9.

9. According to claim 7, wherein the step of performing the user authentication method comprising the step of determining whether the last authentication, based on the face authentication information, the voice authentication information, and the synchronization information.

10.

10. According to claim 9, wherein the face authentication information, the voice authentication information and user authentication method characterized in that at least one of the synchronization information further includes the step of determining when an error is not normal authentication.

11.

11. In the user device, a camera module for acquiring the image; microphone for acquiring a voice; a plurality for obtaining said camera module and a plurality of different biometric information through the microphone, and generates based on the plurality of biometric information using the authentication information, the user device comprising a control unit for processing a single sign-on user.

12.

12. The method of claim 11, wherein the control unit image authentication processing unit for processing the user authentication by the vector detecting the facial feature vector, and the object feature from the image obtained through the camera module; detected vector speech feature from the voice acquired through the microphone to the image processing unit and the user authentication device characterized in that it comprises a certification judgment for processing integrated authentication for the user based on a plurality of authentication information transmitted in the voice authentication processing; by voice authentication processing unit for processing the user authentication.

13.

13. The method of claim 12, wherein the image authentication unit face authentication processing unit for detecting a static the facial feature vector based on the still image captured from said image, processing the face authentication using the detected facial feature vector; the image the user device comprising the object authentication processing for detecting the feature vector and the object, processing the object using the detected authentication object feature vector representing the dynamic state of the object based on the determined.

14.

14. 14. The method of claim 13 wherein the object authentication processing unit operation determination unit that performs user authentication by determining whether motion of an object from the object feature vector, and outputs the operation information in accordance thereto; And said object characterized by using the vector and the speech feature vector two feature vectors are the user device comprises at least one of the synchronization judgment unit judges that it is synchronized in time, outputs the synchronization information over.

15.

15. 15. The method of claim 14 wherein the authentication determination unit authentication face by the authentication of the face authentication processing information, voice authentication information by the authentication of the voice authentication process, and the end certification whether or not based on the operation information by the operation determination unit characterized in that the user device to determine the.

16.

16. 15. The method of claim 14 wherein the authentication determination unit final be authenticated based on the synchronization information by the voice authentication information, and unit the synchronization judgment by the authentication of the face authentication information, the voice authentication processing by the authentication in the face authentication processing characterized in that the user device to determine the.

17.

17. According to claim 11, wherein the user device is a user device comprising a storage section for storing a statistical model for face recognition and voice recognition for the statistical model.

18. And obtaining a plurality of different biometric information for user authentication, and generate respective authentication information for a plurality of biometric information obtained, including a program for performing single sign-on based on the generated authentication information characterized in that the recording medium.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0097581
(43) 공개일자 2013년09월03일

(51) 국제특허분류(Int. Cl.)
G06K 9/46 (2006.01) *G06K 9/20* (2006.01)
(21) 출원번호 10-2012-0019333
(22) 출원일자 2012년02월24일
심사청구일자 없음

(71) 출원인
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
강상기
경기도 수원시 팔달구 인계동 래미안노블클래스아파트 104동 301호
김경태
경기도 화성시 반송동 시범한빛마을KCC스위첼아파트 216동902호
(뒷면에 계속)
(74) 대리인
윤동열

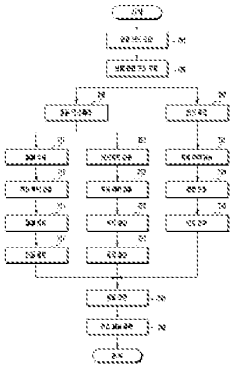
전체 청구항 수 : 총 18 항

(54) 발명의 명칭 **사용자 디바이스에서 복합 생체인식 정보를 이용한 사용자 인증 방법 및 장치**

(57) 요 약

본 발명은 사용자 디바이스에서 사용자의 영상정보 및 음성정보 등과 같은 복합 생체인식 정보(hybrid biometrics information)를 이용하여 사용자를 인증하는 방법 및 그 장치에 관한 것으로, 이러한 본 발명은 사용자 인증 방법에 있어서, 사용자 인증을 위한 서로 다른 복수의 생체인식 정보들을 획득하는 과정; 획득된 복수의 생체인식 정보들에 대한 각각의 인증정보들을 생성하는 과정; 및 생성된 인증정보들을 기반으로 통합 사용자 인증을 수행하는 과정을 포함한다.

대 표 도 - 도7



(72) 발명자

이상훈

서울특별시 관악구 봉천6동 1691-1번지 장미스틴빌라 가동 202호

김양욱

경기도 화성시 석우동 에덴마을 대우푸르지오아파트 162동 2702호

이철환

서울특별시 서초구 서초동 서초자이아파트 101-602

정석영

경기도 용인시 기흥구 영덕동 홍덕힐스테이트 707동 404호

특허청구의 범위

청구항 1

사용자 인증 방법에 있어서,

사용자 인증을 위한 서로 다른 복수의 생체인식 정보들을 획득하는 과정;

획득된 복수의 생체인식 정보들에 대한 각각의 인증정보들을 생성하는 과정;

생성된 인증정보들을 기반으로 통합 사용자 인증을 수행하는 과정을 포함하는 것을 특징으로 하는 사용자 인증 방법.

청구항 2

제1항에 있어서, 상기 획득하는 과정은

카메라 모듈을 통해 영상정보를 획득하는 과정;

마이크를 통해 음성정보를 획득하는 과정을 포함하는 것을 특징으로 하는 사용자 인증 방법.

청구항 3

제2항에 있어서, 상기 생성하는 과정은

상기 영상정보를 기반으로 얼굴 특징벡터 및 오브젝트 특징벡터를 검출하고, 상기 음성정보를 기반으로 음성 특징벡터를 검출하는 과정;

상기 얼굴 특징벡터를 이용한 인증에 대한 얼굴 인증정보를 생성하는 과정;

상기 음성 특징벡터를 이용한 인증에 대한 음성 인증정보를 생성하는 과정;

상기 오브젝트 특징벡터를 이용한 인증에 대한 동작정보를 생성하는 과정을 포함하는 것을 특징으로 하는 사용자 인증 방법.

청구항 4

제3항에 있어서, 상기 동작정보는

설정된 오브젝트의 동작 상태를 나타내는 정보인 것을 특징으로 하는 사용자 인증 방법.

청구항 5

제3항에 있어서, 상기 수행하는 과정은

상기 얼굴 인증정보, 상기 음성 인증정보, 및 상기 동작정보를 기반으로 최종 인증 여부를 결정하는 과정을 포함하는 것을 특징으로 하는 사용자 인증 방법.

청구항 6

제5항에 있어서,

상기 얼굴 인증정보, 상기 음성 인증정보 및 상기 동작정보 중 적어도 하나가 정상 인증되지 않을 시 에러 판정하는 과정을 더 포함하는 것을 특징으로 하는 사용자 인증 방법.

청구항 7

제2항에 있어서, 상기 생성하는 과정은

상기 영상정보를 기반으로 얼굴 특징벡터 및 오브젝트 특징벡터를 검출하고, 상기 음성정보를 기반으로 음성 특징벡터를 검출하는 과정;

상기 얼굴 특징벡터를 이용한 인증에 대한 얼굴 인증정보를 생성하는 과정;

상기 음성 특징벡터를 이용한 인증에 대한 음성 인증정보를 생성하는 과정;

상기 오브젝트 특징벡터와 상기 음성 특징벡터를 이용한 인증에 대한 동기화 정보를 생성하는 과정을 포함하는 것을 특징으로 하는 사용자 인증 방법.

청구항 8

제7항에 있어서, 상기 동기화 정보는

상기 오브젝트 특징벡터와 상기 음성 특징벡터들이 시간적으로 동기화되어 있는지 나타내는 정보인 것을 특징으로 하는 사용자 인증 방법.

청구항 9

제7항에 있어서, 상기 수행하는 과정은

상기 얼굴 인증정보, 상기 음성 인증정보, 및 상기 동기화 정보를 기반으로 최종 인증 여부를 결정하는 과정을 포함하는 것을 특징으로 하는 사용자 인증 방법.

청구항 10

제9항에 있어서,

상기 얼굴 인증정보, 상기 음성 인증정보 및 상기 동기화 정보 중 적어도 하나가 정상 인증되지 않을 시 에러 판정하는 과정을 더 포함하는 것을 특징으로 하는 사용자 인증 방법.

청구항 11

사용자 디바이스에 있어서,

영상을 획득하는 카메라 모듈;

음성을 획득하는 마이크;

상기 카메라 모듈 및 상기 마이크를 통해 서로 다른 복수의 생체인식 정보들을 획득하고, 상기 복수의 생체인식 정보들을 기반으로 생성하는 복수의 인증정보들을 이용하여 사용자에 대한 통합 사용자 인증을 처리하는 제어부를 포함하는 것을 특징으로 하는 사용자 디바이스.

청구항 12

제11항에 있어서, 상기 제어부는

상기 카메라 모듈을 통해 획득된 영상으로부터 얼굴 특징벡터 및 오브젝트 특징벡터 검출에 의한 사용자 인증을 처리하는 영상 인증 처리부;

상기 마이크를 통해 획득된 음성으로부터 음성 특징벡터 검출에 의한 사용자 인증을 처리하는 음성 인증 처리부;

상기 영상 인증 처리부 및 상기 음성 인증 처리부에서 전달되는 복수의 인증정보들을 기반으로 사용자에 대한 통합 인증을 처리하는 인증 판단부를 포함하는 것을 특징으로 하는 사용자 디바이스.

청구항 13

제12항에 있어서, 상기 영상 인증 처리부는

상기 영상으로부터 캡처된 정지영상을 기반으로 검적인 상기 얼굴 특징벡터를 검출하고, 검출된 얼굴 특징벡터를 이용한 얼굴 인증을 처리하는 얼굴 인증 처리부;

상기 영상을 기반으로 결정된 오브젝트의 동적인 상태를 나타내는 상기 오브젝트 특징벡터를 검출하고, 검출된 오브젝트 특징벡터를 이용한 오브젝트 인증을 처리하는 오브젝트 인증 처리부를 포함하는 것을 특징으로 하는 사용자 디바이스.

청구항 14

제13항에 있어서, 상기 오브젝트 인증 처리부는

상기 오브젝트 특징벡터로부터 오브젝트의 동작 여부를 판단하여 사용자 인증을 수행하고, 그에 따른 동작정보를 출력하는 동작 판단부; 및

상기 오브젝트 특징벡터와 상기 음성 특징벡터를 이용하여 두 특징벡터들이 시간적으로 동기화되어 있는지 판단하고, 그에 따른 동기화 정보를 출력하는 동기화 판단부 중 적어도 하나를 포함하는 것을 특징으로 하는 사용자 디바이스.

청구항 15

제14항에 있어서, 상기 인증 판단부는

상기 얼굴 인증 처리부의 인증에 의한 얼굴 인증정보, 상기 음성 인증 처리부의 인증에 의한 음성 인증정보, 및 상기 동작 판단부에 의한 상기 동작정보를 기반으로 최종 인증 여부를 결정하는 것을 특징으로 하는 사용자 디바이스.

청구항 16

제14항에 있어서, 상기 인증 판단부는

상기 얼굴 인증 처리부의 인증에 의한 얼굴 인증정보, 상기 음성 인증 처리부의 인증에 의한 음성 인증정보, 및 상기 동기화 판단부에 의한 상기 동기화 정보를 기반으로 최종 인증 여부를 결정하는 것을 특징으로 하는 사용자 디바이스.

청구항 17

제11항에 있어서, 상기 사용자 디바이스는

얼굴 인식용 통계모델 및 음성 인식용 통계모델을 저장하는 저장부를 포함하는 것을 특징으로 하는 사용자 디바이스.

청구항 18

사용자 인증을 위한 서로 다른 복수의 생체인식 정보들을 획득하고, 획득된 복수의 생체인식 정보들에 대한 각각의 인증정보들을 생성하며, 생성된 인증정보들을 기반으로 통합 사용자 인증을 수행하는 프로그램을 포함하는 것을 특징으로 하는 기록 매체.

명 세 서

기 술 분 야

[0001] 본 발명은 사용자 디바이스에서 사용자 인증 방법 및 장치에 관한 것으로, 특히 사용자 디바이스에서 사용자의 영상정보 및 음성정보 등과 같은 복합 생체인식 정보(hybrid biometrics information)를 이용하여 사용자를 인증하는 방법 및 그 장치에 관한 것이다.

배 경 기 술

[0002] 최근 디지털 기술의 발달과 함께 이동통신 단말기, PDA(Personal Digital Assistant), 전자수첩, 스마트 폰, 태블릿 PC(Personal Computer) 등과 같이 이동하면서 통신 및 개인정보 처리가 가능한 사용자 디바이스들이 다양하게 출시되고 있다. 이러한 사용자 디바이스는 음성 통화, SMS(Short Message Service)/MMS(Multimedia Message Service) 등과 같은 메시지 전송, 영상통화, 전자수첩, 촬영, 이메일 송수신, 방송재생, 동영상재생, 인터넷, 전자상거래, 음악재생, 일정관리, 소셜 네트워크 서비스(SNS, Social Networking Service), 메신저, 사전, 개인과 같이 다양한 기능들을 구비할 수 있다.

[0003] 한편, 사용자 디바이스의 타 사용자로부터 무분별한 사용을 방지하기 위해 보안 기능이 제공되고 있다. 예를 들어, 사용자 디바이스의 턴-온(turn-on) 시 락스크린(lock screen)이 제공되고, 상기 락스크린에서 사용자의 설정된 패스워드(password) 입력에 의해 잠금 기능을 해제하는 등의 기능이 지원되고 있다. 최근 들어서는, 사용자의 지문, 얼굴, 음성, 망막, 그리고 홍채 등과 같은 고유의 신체적 특징을 사용자 인증에 이용하는 생체인식

기술 분야가, 그 뛰어난 보안성을 이유로 새로운 사용자 인증 시스템으로 주목받고 있으며, 그 이용이 급속히 증가하고 있는 추세이다.

[0004] 한편, 기존의 사용자 디바이스에서 사용자의 신체적 특징을 이용한 사용자 인증은 사용자가 사용자 디바이스에 구비된 지문 인식기에 직접 지문정보를 입력하거나, 홍채 인식기에 눈을 밀착시켜야 하는 등 사용자로 하여금 생체인식 정보 입력을 위한 특정 행위를 강요하여 생체인식 정보 입력 시 다소 불편한 문제점이 있었다. 반면, 상기 생체인식 정보 중 얼굴정보 또는 음성정보를 이용하는 경우에는 상기 생체인식 정보 입력 시 사용자가 느끼는 불편함이나 불쾌감을 크게 줄일 수 있는 장점이 있다. 또한 생체인식 정보 인식을 위한 입력장치를 별도로 구비할 필요 없이 사용자 디바이스에서 구비된 카메라모듈 또는 마이크를 그대로 활용할 수 있어 추가 비용을 줄일 수 있다는 장점이 있다. 따라서 상기 생체인식 정보들 중에서도 얼굴 또는 음성 인식을 통한 사용자 인증 기술에 대한 연구가 보다 활발히 진행되고 있다.

발명의 내용

해결하려는 과제

[0005] 본 발명의 목적은 사용자 디바이스에서 복합 생체인식 정보를 이용하여 사용자 인증 시스템을 구현할 수 있는 사용자 인증 방법 및 장치를 제공함에 있다.

[0006] 본 발명의 다른 목적은 사용자 디바이스에서 영상 인증정보와 음성 인증정보를 기반으로 하는 통합적인 사용자 인증에 의해 보안 성능을 높일 수 있는 사용자 인증 방법 및 장치를 제공함에 있다.

[0007] 본 발명의 또 다른 목적은 사용자 디바이스에서 영상 인증정보 및 음성 인증정보를 이용한 사용자 인증 시 얼굴, 입, 눈의 동작 변화를 추가 검출하여 통합적인 사용자 인증을 수행할 수 있는 사용자 인증 방법 및 장치를 제공함에 있다.

[0008] 본 발명의 또 다른 목적은 사용자 디바이스에서 영상 인증정보 및 음성 인증정보를 이용한 사용자 인증 시 입술 동작과 음성 간의 동기화 여부를 추가 판단하여 통합적인 사용자 인증을 수행할 수 있는 사용자 인증 방법 및 장치를 제공함에 있다.

[0009] 본 발명의 또 다른 목적은 사용자 디바이스의 인증모드에서 사용자 인증에 따른 보안 성능을 향상시키기 위한 최적의 환경을 구현하여 사용자의 편의성, 사용자 디바이스의 사용성 및 사용자 디바이스의 경쟁력을 향상시킬 수 있는 방법 및 장치를 제공함에 있다.

과제의 해결 수단

[0010] 상기와 같은 목적들을 달성하기 위한 본 발명의 실시 예에 따른 방법은, 사용자 인증 방법에 있어서, 사용자 인증을 위한 서로 다른 복수의 생체인식 정보들을 획득하는 과정; 획득된 복수의 생체인식 정보들에 대한 각각의 인증정보들을 생성하는 과정; 및 생성된 인증정보들을 기반으로 통합 사용자 인증을 수행하는 과정을 포함한다.

[0011] 상기와 같은 목적들을 달성하기 위하여 본 발명의 실시 예에서는, 상기 방법을 프로세서에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체를 포함한다.

[0012] 상기와 같은 목적들을 달성하기 위한 본 발명의 실시 예에 따른 기록매체는, 사용자 인증을 위한 서로 다른 복수의 생체인식 정보들을 획득하고, 획득된 복수의 생체인식 정보들에 대한 각각의 인증정보들을 생성하며, 생성된 인증정보들을 기반으로 통합 사용자 인증을 수행하는 프로그램을 포함한다.

[0013] 상기와 같은 목적들을 달성하기 위한 본 발명의 실시 예에 따른 장치는, 사용자 디바이스에 있어서, 영상을 획득하는 카메라 모듈; 음성을 획득하는 마이크; 및 상기 카메라 모듈 및 상기 마이크를 통해 서로 다른 복수의 생체인식 정보들을 획득하고, 상기 복수의 생체인식 정보들을 기반으로 생성하는 복수의 인증정보들을 이용하여 사용자에 대한 통합 사용자 인증을 처리하는 제어부를 포함한다.

[0014] 전술한 바와 같은 내용들은 당해 분야 통상의 지식을 가진 자가 후술되는 본 발명의 구체적인 설명으로부터 보다 잘 이해될 수 있도록 하기 위하여 본 발명의 특징들 및 기술적인 장점들을 다소 넓게 약술한 것이다. 이러한 특징들 및 장점들 이외에도 본 발명의 청구범위의 주제를 형성하는 본 발명의 추가적인 특징들 및 장점들이 후술되는 본 발명의 구체적인 설명으로부터 잘 이해될 것이다.

발명의 효과

[0015] 상술한 바와 같이 본 발명에서 제안하는 사용자 디바이스에서 복합 생체인식 정보를 이용한 사용자 인증 방법 및 장치에 따르면, 사용자 디바이스에서 사용자 인증을 위해 단일 생체인식 정보(예컨대, 음성 인식, 얼굴 인식)만을 이용하는 방식보다 보안 성능을 높일 수 있는 이점이 있다. 본 발명에 따르면, 얼굴 인증정보 및 음성 인증정보와 같은 복합 생체인식 정보를 이용한 통합 사용자 인증을 가능하게 하는 이점이 있다. 본 발명에 따르면, 사용자 디바이스에서 영상 인증정보와 음성 인증정보를 기반으로 사용자 인증 시, 상기 사용자 인증 시 얼굴, 입, 눈의 동작 변화를 추가 검출하거나, 입술 동작과 음성 간의 동기화 여부를 추가 판단하는 통합적인 사용자 인증을 수행함으로써, 보안 성능 향상 및 사용자 디바이스가 정당한 사용자에 의해 사용될 수 있도록 유도할 수 있다.

[0016] 본 발명에 따르면, 사용자 인증을 위한 별도의 장치(예컨대, 센서 등)의 구비 없이 사용자 디바이스에 구비되는 카메라 모듈과 마이크를 이용할 수 있다. 그리고 본 발명은 모든 형태의 사용자 디바이스 및 그에 대응하는 다양한 디바이스들에 구현될 수 있다. 또한 본 발명에 따르면 사용자 디바이스에서 사용자 인증을 위한 최적의 환경을 구현하여, 사용자 디바이스의 사용성, 편의성 및 경쟁력을 향상시키는데 기여할 수 있다.

도면의 간단한 설명

[0017] 도 1은 본 발명의 실시 예에 따른 사용자 디바이스의 구성을 개략적으로 도시한 도면이다.

도 2 내지 도 4는 본 발명의 실시 예에 따른 제어부의 구성을 개략적으로 도시한 도면이다.

도 5는 본 발명의 실시 예에 따른 사용자 디바이스에서 복합 생체인식 정보를 이용하여 사용자를 인증하는 동작 예시를 도시한 도면이다.

도 6은 본 발명의 실시 예에 따른 사용자 디바이스에서 사용자 인증을 위한 통계모델 등록 방법을 도시한 흐름도이다.

도 7 및 도 8은 본 발명의 실시 예에 따른 사용자 디바이스에서 사용자 인증 방법을 도시한 흐름도이다.

도 9는 본 발명의 실시 예에 따른 사용자 디바이스에서 사용자 인증을 위한 운용 방법을 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0018] 이하, 첨부된 도면들을 참조하여 본 발명의 바람직한 실시 예들을 상세히 설명한다. 이때, 첨부된 도면들에서 동일한 구성 요소는 가능한 동일한 부호로 나타내고 있음에 유의해야 한다. 또한 본 발명의 요지를 흐리게 할 수 있는 공지 기능 및 구성에 대한 상세한 설명은 생략할 것이다. 즉, 하기의 설명에서는 본 발명의 실시 예에 따른 동작을 이해하는데 필요한 부분만이 설명되며, 그 외의 부분의 설명은 본 발명의 요지를 흐트러지지 않도록 생략될 것이라는 것을 유의하여야 한다.

[0019] 이하에서, 본 발명의 실시 예에 따른 사용자 디바이스의 구성 및 운용 제어 방법에 대하여 하기 도면들을 참조하여 살펴보기로 한다. 본 발명의 실시 예에 따른 사용자 디바이스의 구성 및 운용 제어 방법이 하기에서 기술하는 내용에 제한되거나 한정되는 것은 아니므로 하기의 실시 예에 의거하여 다양한 실시 예들에 적용할 수 있음에 유의하여야 한다. 그리고 이하에서 설명되는 본 발명에서는 하드웨어적인 접근 방법을 예시로서 설명한다. 하지만, 본 발명은 하드웨어와 소프트웨어를 모두 사용하는 기술을 포함하고 있으므로, 본 발명이 소프트웨어 기반의 접근 방법을 제외하는 것은 아니다.

[0020] 도 1은 본 발명의 실시 예에 따른 사용자 디바이스(100)의 구성을 개략적으로 도시한 도면이다.

[0021] 상기 도 1을 참조하면, 본 발명의 사용자 디바이스(100)는 카메라 모듈(110), 오디오처리부(120), 표시부(130), 저장부(140), 그리고 제어부(150)를 포함하여 구성된다. 이 밖에도 상기 사용자 디바이스(100)는 디지털 방송(예컨대, DMB(Digital Multimedia Broadcasting)나 DVB(Digital Video Broadcasting)와 같은 이동 방송)의 수신을 위한 디지털 방송 모듈, 블루투스(Bluetooth) 통신, 적외선(IrDA, Infrared Data Association) 통신, RFID(Radio Frequency Identification) 통신, 그리고 NFC(Near Field Communication) 통신 같은 근거리 무선통신 기반의 통신 기능 지원을 위한 적어도 하나의 근거리 통신 모듈, 하드 키(Hard key) 기반의 입력 지원을 위한 입력부, 이동통신 기반의 음성통화, 영상통화, 데이터통화 등의 통신 기능 지원을 위한 무선통신부, 진동 발생을 위한 진동 발생부, 인터넷 서비스 지원을 위한 무선 랜(LAN, Local Area Network) 모듈, 그리고 상기와 같은 구성들에 전원 공급을 위한 배터리(battery) 등의 구성을 더 포함할 수 있으나, 그들에 대한 설명과 도시는 생략한다.

[0022] 상기 카메라 모듈(110)은 피사체의 정적영상 및 동적영상 촬영을 지원한다. 상기 카메라 모듈(110)은 제어부(180)의 제어에 따라 임의의 피사체를 촬영하고, 촬영된 영상 데이터를 상기 표시부(130) 및 상기 제어부(180)로 전달한다. 상기 카메라 모듈(110)은 입력된 광 신호를 전기적 신호로 변환하는 카메라센서(미도시)와, 상기 카메라센서로부터 입력되는 전기적 신호를 디지털 영상 데이터로 변환하는 신호처리부(미도시) 등을 포함하여 구성될 수 있다. 상기 카메라센서는 CCD(Charge-Coupled Device) 또는 CMOS(Complementary Metal-Oxide-Semiconductor) 등의 방식을 이용하는 센서를 포함할 수 있다. 특히, 본 발명에서 상기 카메라 모듈(110)은 사용자 인증을 위한 인증모드 활성화 시 상기 제어부(180)의 제어 하에 구동되어, 외부의 피사체(예컨대, 사용자의 얼굴 등)에 대한 정적영상 및 동적영상을 촬영하고, 촬영되는 각 영상을 상기 제어부(180)로 전달한다.

[0023] 상기 오디오처리부(120)는 스피커(speaker)(121) 및 마이크(microphone)(123)를 포함하여 구성되고, 사용자 디바이스(100)의 오디오 신호에 대한 입출력을 처리한다. 예를 들어, 상기 오디오처리부(120)는 제어부(180)로부터 입력받은 오디오 신호를 상기 스피커(121)로 전송하고, 상기 마이크(123)로부터 입력받은 음성 등의 오디오 신호를 상기 제어부(180)로 전달하는 기능을 수행한다. 상기 오디오처리부(120)는 음성/음향 데이터를 제어부(180)의 제어에 따라, 상기 스피커(121)를 통해 가청음으로 변환하여 출력하고, 상기 마이크(123)로부터 수신되는 음성 등의 오디오 신호를 디지털 신호로 변환하여 상기 제어부(180)로 전달할 수 있다. 특히, 본 발명에 따른 오디오처리부(120)는 상기 제어부(180)의 제어 하에, 사용자 인증을 위한 인증모드에서 사용자의 음성을 입력받고, 그에 따른 음성신호를 디지털 신호로 변환하여 상기 제어부(180)로 전달한다. 그리고 상기 오디오처리부(120)는 상기 인증모드에서 상기 제어부(180)의 제어 하에, 사용자 인증 과정 진행 시 성공 또는 실패에 대한 효과음 등과 같은 피드백을 상기 스피커(121)로 출력할 수 있다. 상기 인증 성공 또는 실패에 대한 피드백은 사용자 설정에 따라 각각 다양하게 설정될 수 있다.

[0024] 상기 표시부(130)는 사용자 디바이스(100)의 동작 상태 및 관련된 화면을 표시할 수 있다. 예를 들어, 상기 표시부(130)는 사용자 디바이스(100)의 락스크린(lock screen), 홈스크린(home screen), 메뉴스크린(menu screen), 메시지 작성 화면, 채팅 화면, 영상 재생 화면, 및 다양한 어플리케이션들의 실행에 따른 각각의 실행 화면 등을 표시할 수 있다. 그리고 상기 표시부(130)는 사용자 디바이스(100)의 각종 메뉴를 이용하여 사용자가 입력한 정보 또는 사용자에게 제공되는 정보를 표시한다. 즉, 상기 표시부(130)는 사용자 디바이스(100) 이용에 따른 다양한 사용자 기능의 실행화면을 제공할 수 있다. 상기 표시부(130)는 액정표시장치(LCD, Liquid Crystal Display)가 사용되는 것이 일반적이나, 발광다이오드(LED, Light Emitting Diode), 유기발광다이오드(OLED, Organic LED), 그리고 능동형 OLED(AMOLED, Active Matrix OLED) 등과 같은 다른 표시장치가 사용될 수도 있다. 또한 상기 표시부(130)는 휘어질 수 있는 플렉서블 디스플레이(flexible display)로 구현될 수 있다. 상기 플렉서블 디스플레이는 종이처럼 얇고 유연한 기판을 통해 손상 없이 휘기나 구부리거나 말 수 있는 장치를 나타낸다. 또한 상기 표시부(130)는 터치(touch) 기반의 입력을 지원하는 인터페이스(interface)를 포함하여 구성될 수 있다. 예를 들어, 상기 표시부(130)는 터치스크린(touchscreen) 구성에 의해 터치 기반의 다양한 사용자 입력을 지원하고, 사용자 입력에 따른 입력신호를 생성하여 상기 제어부(180)로 전달할 수 있다. 또한 상기 표시부(130)는 앞서와 같은 다양한 화면을 표시할 시 사용자 디바이스(100)의 회전 방향(또는 놓인 방향)에 따라 가로모드에 의한 화면 표시, 세로모드에 의한 화면 표시 및 가로모드와 세로모드 간의 변화에 따른 적응적 화면 전환 표시를 지원할 수 있다. 특히, 상기 표시부(130)는 사용자 디바이스(100)의 사용자 인증을 위한 인증모드에서 상기 제어부(180)의 제어에 따라 제공되는 특정 영상을 표시할 수 있다. 예를 들어, 상기 표시부(130)는 인증모드에서 상기 카메라 모듈(110)을 통해 촬영되는 사용자의 얼굴정보를 표시할 수 있다.

[0025] 상기 저장부(140)는 사용자 디바이스(100)에서 운용되는 각종 어플리케이션과 데이터를 저장하며, 하나 이상의 비휘발성 메모리(non-volatile memory)와 휘발성 메모리(volatile memory)를 포함하여 구성될 수 있다. 상기 저장부(140)는 ROM(Read Only Memory), 플래시 메모리(flash memory), RAM(Random Access Memory), 내장 하드디스크(HDD, Hard Disk), 외장 하드디스크, 메모리카드(memory card)와 같은 외부 저장매체 등 중 적어도 하나로 구성될 수 있다. 그리고 상기 저장부(140)는 상기 사용자 디바이스(100)의 운영체제, 상기 표시부(130)의 표시 제어 동작과 관련된 프로그램과 데이터, 인증모드에서 복합 생체인식 정보(예컨대, 얼굴정보 및 음성정보)를 이용한 사용자 인증 기능 운용과 관련된 프로그램과 데이터 등을 저속적으로 또는 일시적으로 저장할 수 있다. 특히, 상기 저장부(140)는 본 발명의 실시 예에 따라 인증모드에서 상기 카메라 모듈(110)을 통해 촬영되는 영상과 관련된 데이터를 정적데이터와 동적데이터로 각각 저장할 수 있다. 그리고 상기 저장부(140)는 상기 인증모드에서 사용자 인증을 위해 입력되는 생체인식 정보를 식별하기 위한 학습정보를 학습정보 저장영역(150)에 저장할 수 있다. 상기 학습정보는 얼굴정보와 음성정보로 구분될 수 있으며, 각각의 할당된 저장영역에 저장될 수 있다. 상기 얼굴정보는 인증모드에서 인증된 사용자의 영상에서 소정의 얼굴 특징을 추출하고, 추출된 상기

얼굴 특징을 기초로 얼굴 특징벡터(feature vector)를 생성하여 얼굴 인식용 통계모델로 얼굴정보 저장영역(160)에 등록될 수 있다. 상기 음성정보는 인증모드에서 인증될 사용자의 음성에서 소정의 음성 특징을 추출하고, 추출된 상기 음성 특성을 기초로 음성 특징벡터를 생성하여 음성 인식용 통계모델로 음성정보 저장영역(170)에 등록될 수 있다.

[0026] 그리고 상기 저장부(140)는 프로그램 영역과 데이터 영역을 포함할 수 있다. 상기 프로그램 영역은 사용자 디바이스(100)의 부팅 및 상기한 바와 같은 각 구성들의 운용을 위한 운영 체제와, 다운로드 및 설치된 어플리케이션들 등을 저장할 수 있다. 상기 데이터 영역은 사용자 디바이스(100)의 사용에 따라 발생하는 데이터가 저장되는 영역을 나타낸다. 상기 데이터 영역은 실행되는 어플리케이션에 따라 사용되거나 생성되는 데이터를 저장하며, 인증모드에서 입력되는 영상데이터 및 음성데이터를 버퍼링 또는 저장할 수 있다.

[0027] 상기 제어부(180)는 사용자 디바이스(100)의 전반적인 동작을 제어한다. 특히, 상기 제어부(180)는 사용자 디바이스(100)의 인증모드에서 얼굴정보 및 음성정보와 같은 복합 생체인식 정보를 이용한 사용자 인증과 관련된 동작을 제어할 수 있다. 상기 제어부(180)는 인증 모드에서 얼굴 인식 결과, 음성 인식 결과, 오브젝트 판단 결과, 및 동기화 판단 결과와 같은 복합적인 정보들을 기반으로 사용자에 대한 통합 인증을 처리할 수 있다. 그리고 제어부(180)는 복합적인 정보들 중 어느 하나로도 비인증된 사용자임이 확인될 시 사용자 인증에 대해 에러 판정할 수 있다. 예를 들어, 상기 각 결과들은 미리 정의된 기준 확률 값(예컨대, 80%, 85%, 90% 등)을 충족하는지 여부에 대응하여 인증된 사용자임을 통지하는 결과가 출력되거나 비인증된 사용자임을 통지하는 결과가 출력될 수 있다. 따라서 제어부(180)는 상기 각 결과들의 개별 확률 값 충족 여부를 통해 에러 판정 여부를 결정할 수 있다.

[0028] 상기 제어부(180)는 도시 영상 인증 처리부(10), 음성 인증 처리부(40), 통계모델 관리부(50), 그리고 인증 판단부(200)를 포함하여 구성된다. 상기 제어부(180)는 본 발명의 기능 운용에 대한 전반적인 동작을 제어할 수 있으며, 이러한 제어부(180)의 상세 제어 동작에 대해 후술하는 도면들을 참조한 사용자 디바이스(100)의 동작 예시 및 그의 제어 방법에서 설명될 것이다.

[0029] 한편, 상기 제어부(180)는 본 발명의 기능 외에 상기 사용자 디바이스(100)의 통상적인 기능과 관련된 각종 동작을 제어할 수 있다. 예를 들어, 상기 제어부(180)는 터치 기반의 입력 인터페이스를 통해 입력되는 터치 이벤트에 응답하여, 그에 따른 기능 운용을 제어할 수 있다. 또한 상기 제어부(180)는 유선통신 기반 또는 무선통신 기반으로 각종 데이터의 송수신을 제어할 수 있다. 그리고 상기 제어부(180)는 CPU(Central Processing Unit), GPU(Graphical Processing Unit), 및 메모리 등이 하나의 칩(chip) 안에 내장되는 시스템 온 칩(SoC, System on Chip)으로 구현될 수 있다. 상기 SoC의 각 구성은 시스템 버스(system bus)로 연결되어 그들 간의 데이터 통신이 이루어질 수 있다. 또는 상기 제어부(180)는 CPU, GPU 및 메모리 등이 멀티 레이어(multi layer)로 패키징(packaging)된 것일 수 있다.

[0030] 그리고 상기 도 1에 나타낸 본 발명의 사용자 디바이스(100)는 본 발명의 사용자 인증 기술을 지원하기 위한 구조를 가지는 모든 정보통신기기, 멀티미디어기기 및 그에 대한 응용기기를 포함할 수 있다. 예를 들어, 상기 사용자 디바이스(100)는 다양한 통신 시스템에 대응되는 각 통신 프로토콜들(communication protocols)에 의거하여 동작하는 이동통신 단말기를 비롯하여, 태블릿 PC(Personal Computer), 스마트 폰(Smart Phone), 디지털 카메라, PMP(Portable Multimedia Player), 미디어 플레이어(Media Player), 휴대게임단말 및 PDA(Personal Digital Assistant) 등의 디바이스를 포함할 수 있다. 아울러, 본 발명의 방법은 디지털 TV(Digital Television), DS(Digital Signage), LFD(Large Format Display), 랩톱 컴퓨터 등과 같이 다양한 디바이스에 적용되어 운용될 수 있다.

[0031] 도 2는 본 발명의 실시 예에 따른 제어부(180)의 구성을 개략적으로 도시한 도면이다.

[0032] 상기 도 2를 참조하면, 본 발명의 제어부(180)는 상기 카메라 모듈(110)을 통해 획득된 영상으로부터 얼굴 특징벡터 및 오브젝트 특징벡터 검출에 의한 사용자 인증을 처리하는 영상 인증 처리부(10), 상기 마이크(123)를 통해 획득된 음성으로부터 음성 특징벡터 검출에 의한 사용자 인증을 처리하는 음성 인증 처리부(40), 그리고 상기 영상 인증 처리부(10) 및 상기 음성 인증 처리부(40)에서 전달되는 복수의 인증정보들(예컨대, 얼굴 인증정보, 음성 인증정보 등)을 기반으로 상기 사용자에 대한 통합 인증을 처리하는 인증 판단부(200)를 포함하여 구성된다. 그리고 상기 영상 인증 처리부(10)는 획득된 영상으로부터 캡쳐(capture)된 정지영상을 기반으로 정적인 특징벡터 검출에 의한 얼굴 인증을 처리하는 얼굴 인증 처리부(20)와, 획득된 영상을 기반으로 특정 오브젝트(예컨대, 얼굴, 눈, 입술 등)의 동적인 특징벡터 검출에 의한 오브젝트 인증을 처리하는 오브젝트 인증 처리부(30)를 포함하여 구성된다. 본 발명에서 상기 오브젝트는 인식된 영상에서 얼굴의 특정 영역을 구분한

것으로, 앞서와 같이 얼굴 자체, 눈, 입술 등을 포함할 수 있다. 그리고 상기 오브젝트로부터 검출되는 오브젝트 특징벡터는 얼굴의 움직임, 눈의 깜박임, 입술의 움직임 등의 동적인 특징벡터가 검출될 수 있다.

[0033] 상기 얼굴 인증 처리부(20)는 얼굴 추출부(210), 제1 특징벡터 검출부(220), 그리고 얼굴 인증부(230)를 포함하여 구성된다.

[0034] 상기 얼굴 추출부(210)는 상기 카메라 모듈(110)을 통해 입력되는 영상으로부터 사용자의 얼굴을 추출한다. 예를 들어, 상기 얼굴 추출부(210)는 입력된 얼굴 영상으로부터 얼굴 영역, 눈 영역, 그리고 입 영역 등의 특성을 추출하여 출력할 수 있다. 본 발명에서 상기 얼굴 검출부(210)는 상기 카메라 모듈(110)로부터 입력되어 상기 표시부(130)를 통해 표시되는 영상을 캡처하고, 캡처된 정지영상을 통해 사용자의 얼굴 인식 및 얼굴 특징 추출을 수행할 수 있다.

[0035] 상기 제1 특징벡터 검출부(220)는 상기 얼굴 추출부(210)에서 추출된 특징으로부터 얼굴 특징벡터(예컨대, 얼굴의 눈, 코, 입 간에 점을 찍어 형성되는 거리와 각도, 및 피부색 등)를 검출할 수 있다. 예를 들어, 상기 제1 특징벡터 검출부(220)는 상기 얼굴 추출부(210)에서 추출된 특징 중 눈의 중심점 등을 이용하여 얼굴 영상에 대한 정규화를 수행하고, 정규화된 얼굴 영상에서 얼굴의 고유한 얼굴 특징벡터를 추출하여 출력한다.

[0036] 상기 얼굴 인증부(230)는 상기 제1 특징벡터 검출부(220)에서 추출된 얼굴의 고유한 특징인 상기 얼굴 특징벡터를 미리 등록된 얼굴정보(특히, 얼굴 인식용 통계모델)와 비교하여 얼굴 영상에 대한 인증을 수행하고, 인증 결과에 따른 인증정보를 출력한다. 예를 들어, 상기 얼굴 인증부(230)는 상기 추출된 얼굴 특징벡터와 미리 학습되어 저장된 상기 얼굴정보를 비교하고, 그들 간의 일치 여부를 판별할 수 있다. 이때, 상기 일치 여부 판별을 위한 설정된 오차범위를 감안하여 판별될 수 있으며, 예컨대, 90% 이상 일치 시 인증된 사용자임을 나타내는 인증정보를 출력할 수 있다. 반면, 90% 미만 일치(얼굴 특징벡터가 없는 경우 즉, 얼굴이 촬영되지 않은 경우 포함) 시 비인증된 사용자임을 나타내는 인증정보를 출력할 수 있다. 상기 일치 여부를 판별을 위한 기준 확률 값은 상기 90%를 비롯하여 사용자 설정에 따라 80%, 85% 등과 같이 다양하게 설정될 수 있다.

[0037] 상기 오브젝트 인증 처리부(30)는 오브젝트 검출부(240), 제2 특징벡터 검출부(250), 그리고 동작 판단부(260)를 포함하여 구성된다. 본 발명에서 상기 오브젝트 인증 처리부(30)는 카메라 모듈(110)에서 입력되는 영상(특히, 동영상)을 통해 오브젝트(예컨대, 얼굴, 눈, 입 등)를 검출하여 상기 오브젝트의 움직임 여부를 판별하는 동작 인식부에 해당할 수 있다.

[0038] 상기 오브젝트 검출부(240)는 상기 카메라 모듈(110)을 통해 입력되는 영상으로부터 오브젝트를 추출한다. 본 발명에서 상기 오브젝트는 사용자의 얼굴에서 움직임을 판별하기 위한 요소로, 얼굴, 눈, 입 등에 해당할 수 있다. 예를 들어, 상기 오브젝트 검출부(240)는 입력된 얼굴 영상으로부터 얼굴 영역, 눈 영역, 그리고 입 영역 중 설정된 오브젝트의 영역을 추출하여 출력할 수 있다. 즉, 상기 오브젝트 검출부(240)는 상기 카메라 모듈(110)로부터 입력되어 상기 표시부(130)를 통해 표시되는 영상에서 설정된 오브젝트의 위치를 검출할 수 있다.

[0039] 상기 제2 특징벡터 검출부(250)는 상기 오브젝트 검출부(240)에서 검출된 오브젝트의 위치에서 상기 오브젝트의 동작(움직임)을 나타내는 오브젝트 특징벡터(예컨대, 얼굴의 움직임, 눈의 깜박임, 입의 움직임 등)를 검출할 수 있다. 예를 들어, 상기 제2 특징벡터 검출부(250)는 상기 오브젝트 검출부(240)에서 추출된 특징 중 입의 움직임에 따라 변화되는 입술의 크기, 입술의 모양 등을 기반으로 하는 특징벡터를 추출하여 출력할 수 있다. 또는 상기 제2 특징벡터 검출부(250)는 상기 오브젝트 검출부(240)에서 추출된 특징 중 눈 모양의 변화(눈의 깜박임에 대응)되는 특징벡터를 추출하여 출력할 수 있다. 또는 상기 제2 특징벡터 검출부(250)는 상기 오브젝트 검출부(240)에서 추출된 특징 중 얼굴의 움직임에 따라 얼굴의 크기 변화, 얼굴의 위치 변화 등의 특징벡터를 추출하여 출력할 수 있다.

[0040] 상기 동작 판단부(260)는 상기 제2 특징벡터 검출부(250)에서 검출된 상기 오브젝트 특징벡터로부터 해당 오브젝트의 동작(움직임) 여부를 판단하여 사용자에 대한 인증을 수행하고, 인증 결과에 따른 동작정보(인증정보)를 출력한다. 예를 들어, 상기 동작 판단부(250)는 오브젝트의 움직임이 있는 것으로 판단할 시 동작이 있음을 나타내는 동작정보를 출력할 수 있다. 반면, 상기 동작 판단부(250)는 오브젝트의 움직임이 없는 것으로 판단할 시 동작이 없음을 나타내는 동작정보를 출력할 수 있다.

[0041] 상기 음성 인증 처리부(40)는 제3 특징벡터 검출부(270) 및 음성 인증부(280)를 포함하여 구성된다.

[0042] 상기 제3 특징벡터 검출부(270)는 상기 마이크(123)를 통해 입력되는 음성으로부터 음성 특성벡터(예컨대, 톤(tone), 주파수(frequency), 어휘, 속도 등)를 검출하여 출력할 수 있다. 이때, 상기 제3 특징벡터 검출부(270)는 음성 인증의 운용 방식에 따라 적어도 하나의 특징벡터를 검출할 수 있다. 예를 들어, 음성 인증을 위한

운용 방식이 사용자가 말하는 어휘에 관계없이 운용되는 방식(예컨대, 사용자가 말하는 단어와는 무관하게 문어나 주파수만을 구분하는 인증 방식)인 경우, 상기 제3 특징벡터 검출부(270)는 음성의 톤, 주파수, 속도 등의 특징벡터 중 설정된 적어도 하나의 특징벡터를 검출할 수 있다. 또는 음성 인증을 위한 운용 방식이 사용자가 말하는 어휘를 구분하여 운용되는 방식(예컨대, 미리 설정된 단어 입력을 요하는 인증 방식)인 경우, 상기 제3 특징벡터 검출부(270)는 음성의 톤, 주파수, 속도의 특징벡터 중 설정된 적어도 하나의 특징벡터와 상기 음성으로부터 구분되는 어휘의 특징벡터를 함께 검출할 수 있다.

[0043] 상기 음성 인증부(280)는 상기 제3 특징벡터 검출부(270)에서 검출된 음성의 고유한 특성인 상기 음성 특징벡터를 미리 등록된 음성정보(특히, 음성 인식용 통계모델)와 비교하여 음성에 대한 인증을 수행하고, 인증 결과에 따른 인증정보를 출력한다. 예를 들어, 상기 음성 인증부(280)는 상기 검출된 음성 특징벡터와 미리 학습되어 저장된 상기 음성정보를 비교하고, 그들 간의 일치 여부를 판별할 수 있다. 이때, 상기 일치 여부 판별은 설정된 오차범위를 감안하여 판별될 수 있으며, 예컨대, 90% 이상 일치 시 인증된 사용자임을 나타내는 인증정보를 출력할 수 있다. 반면, 90% 미만 일치(음성 특징벡터가 없는 경우 즉, 음성이 입력되지 않은 경우 포함) 시 비인증된 사용자임을 나타내는 인증정보를 출력할 수 있다. 상기 일치 여부 판별을 위한 기준 확률 값은 상기 90%를 비롯하여 사용자 설정에 따라 80%, 85% 등과 같이 다양하게 설정될 수 있다.

[0044] 그리고 상기 음성 인증부(280)는 음성 인증의 운용 방식에 따라 적어도 하나의 특징벡터를 이용한 인증을 수행할 수 있다. 예를 들어, 음성 인증을 위한 운용 방식이 사용자가 말하는 어휘에 관계없이 운용되는 방식인 경우, 상기 음성 인증부(280)는 상기 제3 특징벡터 검출부(270)에서 검출되어 전달되는 특징벡터와 미리 학습된 음성정보 중 상기 특징벡터에 대응하는 특징벡터만을 비교하여 그의 인증을 수행할 수 있다. 반면, 음성 인증을 위한 운용 방식이 사용자가 말하는 어휘를 구분하여 운용되는 방식인 경우, 상기 음성 인증부(280)는 상기 제3 특징벡터 검출부(270)에서 전달되는 특징벡터들 중 어휘 특징벡터와 미리 학습된 음성정보(특히, 어휘 특징벡터)를 비교하여 인증을 수행(예컨대, 입력된 단어와 학습된 단어가 일치하는지 판정)할 수 있다. 즉, 상기 음성 인증부(280)는 인식된 어휘 특징벡터를 훈련된 어휘 특징벡터와 비교하여 입력된 음성의 어휘에 대한 인증을 수행할 수 있다. 그리고 상기 음성 인증부(280)는 상기 어휘 특징벡터에 대한 인증이 통과할 시 상기 제3 특징벡터 검출부(270)에서 전달되는 다른 특징벡터(예컨대, 톤, 주파수, 속도 중 적어도 하나)와 미리 학습된 음성정보(특히, 톤, 주파수, 속도 중 적어도 하나)를 비교하여 그의 인증을 수행할 수 있다. 이러한 음성 인증 방식은 사용자 설정에 따라 다양하게 운용될 수 있다.

[0045] 상기 인증 판단부(290)는 상기 얼굴 인증 처리부(20)에서 전달되는 얼굴 인증정보, 상기 오브젝트 인증 처리부(30)에서 전달되는 동작정보, 그리고 상기 음성 인증 처리부(40)에서 전달되는 음성 인증정보를 이용하여 통합 인증을 수행하고 그에 따른 인증 결과를 출력할 수 있다. 상기 인증 판단부(290)는 전달된 얼굴 인증정보, 동작정보, 그리고 음성 인증정보를 분석하여 모두 인증된 사용자임을 나타낼 시 사용자 인증을 정상 처리할 수 있다. 또는 상기 인증 판단부(290)는 전달된 얼굴 인증정보, 동작정보, 그리고 음성 인증정보를 분석하여 어느 하나라도 비인증된 사용자임을 나타낼 시 사용자 인증을 에러 처리할 수 있다. 예를 들어, 상기 인증 판단부(290)는 얼굴 인증정보를 통해 인증된 사용자 얼굴임을 확인하고, 음성 인증정보를 통해 인증된 사용자 음성임을 확인하고, 동작정보를 통해 결정된 오브젝트의 동작 상태를 확인할 시 사용자 인증을 정상 처리할 수 있다. 반면, 상기 인증 판단부(290)는 얼굴 인증정보를 통해 비인증된 사용자 얼굴임을 확인하거나, 음성 인증정보를 통해 비인증된 사용자 음성임을 확인하거나, 또는 동작정보를 통해 결정된 오브젝트의 비동작 상태를 확인할 시 사용자 인증을 에러 처리할 수 있다.

[0046] 도 3은 본 발명의 실시 예에 따른 제어부(180)의 구성을 개략적으로 도시한 도면이다.

[0047] 상기 도 3을 참조하면, 본 발명의 제어부(180)는 상기 카메라 모듈(110)을 통해 획득된 영상으로부터 얼굴 특징벡터 검출에 의한 사용자 인증을 처리하는 영상 인증 처리부(10), 상기 마이크(123)를 통해 획득된 음성으로부터 음성 특징벡터 검출에 의한 사용자 인증을 처리하는 음성 인증 처리부(40), 그리고 상기 영상 인증 처리부(10) 및 상기 음성 인증 처리부(40)에서 전달되는 각각의 인증정보들(예컨대, 얼굴 인증정보, 음성 인증정보 등)을 기반으로 상기 사용자에 대한 통합 인증을 처리하는 인증 판단부(290)를 포함하여 구성된다. 그리고 상기 영상 인증 처리부(10)는 획득된 영상으로부터 웹캠과 정지영상을 기반으로 정적인 특징벡터 검출에 의한 얼굴 인증을 처리하는 얼굴 인증 처리부(20)와, 획득된 영상을 기반으로 특정 오브젝트(예컨대, 얼굴, 눈, 입술 등)의 동적인 특징벡터 검출에 의한 오브젝트 인증을 처리하는 오브젝트 인증 처리부(30)를 포함하여 구성된다.

[0048] 상기 도 3에 도시된 바와 같이, 본 발명의 다른 실시 예에 따른 상기 제어부(180)의 구성은 앞서 도 2를 참조한 제어부(180)의 구성 중 동작 판단부(260)의 구성이 생략되고 동기화 판단부(300)가 포함되며, 그에 따라 인증

판단부(290)의 통합 인증 방식이 달라지는 것에 있다. 따라서 앞서 도 2를 참조한 설명 부분에서 동일한 구성에 대해서는 참조번호가 일치하며, 중복되는 설명은 생략하도록 한다. 그리고 본 발명에서는 상기 도 2의 제어부(180)의 구성과 상기 도 3의 제어부(180)의 구성을 구분하여 나타내었으나, 상기 통합 판단부(260)의 동작과 상기 동기화 판단부(300)의 동작을 하나의 구성으로 결합하여 운용될 수 있으며, 또는 상기 제어부(180) 내에 상기 두 개의 구성이 모두 구성될 수 있음은 물론이다. 이하, 상기 도 3의 제어부(180)의 구성에서 상기 도 2의 제어부(180)의 구성과 차이나는 부분에 대해서 설명한다.

[0049] 상기 오브젝트 인증 처리부(30)의 상기 제2 특징벡터 검출부(250)는 상기 오브젝트 검출부(240)에서 검출된 오브젝트의 위치에서 상기 오브젝트의 동작(움직임)을 나타내는 오브젝트 특징벡터(예컨대, 얼굴의 움직임, 눈의 깜박임, 입의 움직임 등)를 검출하여 출력할 수 있다. 특히, 상기 도 3에서는 상기 오브젝트가 입인 경우를 나타내며, 따라서 입의 움직임에 따라 입술의 크기 변화, 입술의 모양 변화 등에 따른 오브젝트 특징벡터를 검출하여 상기 동기화 판단부(300)로 출력하는 것을 예시로 설명한다.

[0050] 그리고 상기 음성 인증 처리부(40)의 상기 제3 특징벡터 검출부(270)는 앞서 설명한 바와 같이 상기 마이크(123)를 통해 입력되는 음성으로부터 음성 특징벡터(예컨대, 톤, 주파수, 어휘, 속도 등)를 검출하여 출력할 수 있다. 이때, 상기 제3 특징벡터 검출부(270)는 상기 검출된 음성 특징벡터를 상기 음성 인증부(280)를 비롯하여 상기 동기화 판단부(300)로 각각 출력할 수 있다.

[0051] 한편, 상기 동기화 판단부(300)는 상기 제2 특징벡터(250)에서 전달되는 오브젝트 특징벡터와 상기 제3 특징벡터(270)에서 전달되는 음성 특징벡터를 이용하여, 상기 두 특징벡터들이 시간적으로 동기화되어 있는지 판단하고, 그에 따른 동기화 정보를 출력한다. 예를 들어, 상기 동기화 판단부(300)는 상기 오브젝트 특징벡터에 따른 입술의 움직이는 동작과 상기 음성 오브젝트에 따른 음성의 동적 특성을 비교하고, 두 특성이 동기화되어 있는지 여부를 판단할 수 있다. 여기서, 상기 동기화 판단은 이미 훈련된 통계모델(예컨대, 입술 동작과 음성에 대해 학습된 통계모델)을 통해 입술 오브젝트가 동적인 특징벡터를 가지고, 그에 대응하여 음성 특징벡터가 검출되는지를 판단하는 방식으로 이루어질 수 있다. 또는 상기 동기화 판단은 상기 통계모델 없이 입술 오브젝트의 특징벡터를 기반으로 소리를 내어 말을 하는 현실적인 언어 행위 즉, 발화(utterance)의 시작점과 끝점을 검출하고, 상기 음성 특징벡터를 기반으로 발화의 시작점과 끝점을 검출하여, 두 개의 검출된 값을 비교하는 방식으로 이루어질 수 있다.

[0052] 상기 인증 판단부(290)는 상기 얼굴 인증 처리부(20)에서 전달되는 얼굴 인증정보, 상기 동기화 판단부(300)에서 전달되는 동기화 정보, 그리고 상기 음성 인증 처리부(40)에서 전달되는 음성 인증정보를 이용하여 통합 인증을 수행하고 그에 따른 인증 결과를 출력할 수 있다. 상기 인증 판단부(290)는 전달된 얼굴 인증정보, 동기화 정보, 그리고 음성 인증정보를 분석하여 모두 인증된 사용자임을 나타낼 시 사용자 인증을 정상 처리할 수 있다. 또는 상기 인증 판단부(290)는 전달된 얼굴 인증정보, 동기화 정보, 그리고 음성 인증정보를 분석하여 어느 하나라도 비인증된 사용자임을 나타낼 시 사용자 인증을 에러 처리할 수 있다. 예를 들어, 상기 인증 판단부(290)는 얼굴 인증정보를 통해 인증된 사용자 얼굴임을 확인하고, 음성 인증정보를 통해 인증된 사용자 음성임을 확인하고, 동기화 정보를 통해 오브젝트 특징벡터와 음성 특징벡터 간의 동기화가 일치하는 것을 확인할 시 사용자 인증을 정상 처리할 수 있다. 반면, 상기 인증 판단부(290)는 얼굴 인증정보를 통해 비인증된 사용자 얼굴임을 확인하거나, 음성 인증정보를 통해 비인증된 사용자 음성임을 확인하거나, 또는 동기화 정보를 통해 오브젝트 특징벡터와 음성 특징벡터 간의 동기화가 일치하지 않는 것을 확인할 시 사용자 인증을 에러 처리할 수 있다.

[0053] 도 4는 본 발명의 실시 예에 따른 제어부(180)에서 통계모델 관리부(50)의 구성을 개략적으로 도시한 도면이다.

[0054] 상기 도 4를 참조하면, 본 발명의 통계모델 관리부(50)는 얼굴인증 학습부(410), 음성인증 학습부(420), 그리고 학습정보 처리부(430)를 포함하여 구성된다.

[0055] 상기 얼굴인증 학습부(410)는 앞서 살펴본 바와 같은 영상 인증 처리부(10)를 통해 처리되는 얼굴의 특징벡터를 기반으로 하여 얼굴 인식용 통계모델을 생성하여 출력할 수 있다.

[0056] 상기 음성인증 학습부(420)는 앞서 살펴본 바와 같은 음성 인증 처리부(40)를 통해 처리되는 음성의 특징벡터를 기반으로 하여 음성 인식용 통계모델을 생성하여 출력할 수 있다.

[0057] 상기 학습정보 처리부(430)는 인증 모드에서 검출되는 얼굴 특징벡터, 오브젝트 특징벡터, 및 음성 특징벡터에 대한 사용자 인증을 위해, 상기 얼굴 인식용 통계모델과 상기 음성 인식용 통계모델을 상기 저장부(140)에 저장할 수 있다. 상기 학습정보 처리부(430)는 반복 학습된 얼굴 인식용 통계모델과 음성 인식용 통계모델을 기반으

로 얼굴정보 및 음성정보로 각각의 할당된 저장영역에 저장할 수 있다. 이때, 상기 얼굴정보의 경우 학습된 얼굴 인식용 통계모델에 따라 얼굴의 특징벡터 및 오브젝트의 특징벡터로 구분되어 관리될 수 있다. 그리고 상기 음성정보의 경우 학습된 음성 인식용 통계모델에 따라 음성의 고유한 톤, 주파수, 속도 등과 같은 특징벡터와 보안 인증용 어휘(예컨대, 패스워드에 대응하는 단어 등)와 같은 특징벡터로 구분되어 관리될 수 있다.

[0058] 도 5는 본 발명의 실시 예에 따른 사용자 디바이스(100)에서 복합 생체인식 정보를 이용하여 사용자를 인증하는 동작 예시를 도시한 도면이다.

[0059] 특히, 상기 도 5에서는 사용자 디바이스(100)의 락스크린을 해제하기 위해 인증 모드가 활성되는 경우의 예시를 나타낸 것이다.

[0060] 상기 도 5를 참조하면, 참조번호 <501>에 도시된 바와 같이 사용자 디바이스(100)가 대기모드에 따라 표시부(130)가 턴-오프(turn-off) 상태에서, 사용자의 조작(표시부(130)의 턴-온(turn-on)을 위한 사용자의 핫키(hot key) 입력 행위 등)에 의해 참조번호 <503>에 도시된 바와 같이 표시부(130)가 턴-온 될 수 있다. 이때, 상기 도 5에서는 사용자 디바이스(100)의 보호를 위해 사용자의 잠금 기능 설정 및 그에 대한 락스크린이 설정된 경우를 가정한다. 따라서 상기 표시부(130)가 턴-오프 상태에서 턴-온 상태로 전환될 시, 제어부(180)는 상기 참조번호 <503>에 나타낸 바와 같이 사용자에 의해 설정된 락스크린을 상기 표시부(130)에 나타낼 수 있다.

[0061] 다음으로, 제어부(180)는 상기 참조번호 <503>과 같이 락스크린을 제공할 시 사용자의 인증을 위한 인증 모드가 설정되어 있는지 판별할 수 있다. 그리고 제어부(180)는 상기 인증 모드가 설정된 경우 카메라 모듈(110)과 마이크(123)를 구동하고 인증 모드를 실행할 수 있다.

[0062] 다음으로, 제어부(180)는 참조번호 <505>에 나타낸 바와 같이 상기 카메라 모듈(110)을 통해 획득된 영상을 상기 표시부(130)에 나타낼 수 있다. 예를 들어, 사용자는 상기 표시부(130) 턴-온 시 상기 카메라 모듈(110)(특히, 전면 카메라)을 통해 사용자 얼굴이 촬영될 수 있도록 사용자 디바이스(100)를 공간상에 위치시킬 수 있다. 그러면, 제어부(180)는 상기 카메라 모듈(110)을 통해 입력되는 영상(특히, 사용자 얼굴 영상)을 표시부(130)로 전달하여 그를 표시할 수 있다. 이때, 제어부(180)는 표시부(130)에 표시된 락스크린 상의 일 영역에 상기 카메라 모듈(110)을 통해 입력되는 영상을 오버레이(overlay)하여 나타낼 수 있다. 또는 제어부(180)는 락스크린 표시는 생략하고 상기 카메라 모듈(110)을 통해 입력되는 영상만을 나타낼 수도 있다.

[0063] 다음으로, 사용자는 상기 참조번호 <505>에 나타낸 바와 같이 상기 표시부(130)를 통해 사용자의 얼굴이 나타나면 음성을 발화할 수 있다. 그러면, 상기 표시부(130)에서는 참조번호 <505> 내지 참조번호 <509>에 나타낸 바와 같이 사용자의 발화에 따라 변화되는 영상이 나타날 수 있다. 이때, 제어부(180)는 상기 카메라 모듈(110)을 통해 입력되는 영상을 표시부(130)를 통해 표시하면서, 상기 입력되는 영상으로부터 사용자 인증을 위한 특징벡터(예컨대, 얼굴 특징벡터 및 오브젝트 특징벡터)를 검출할 수 있다. 또한 제어부(180)는 마이크(123)를 통해 입력되는 음성으로부터 사용자 인증을 위한 특징벡터(예컨대, 음성역 톤, 주파수, 어휘, 소리 등)를 검출할 수 있다.

[0064] 다음으로, 제어부(180)는 상기 카메라 모듈(110)의 입력 영상으로부터 검출된 얼굴 특징벡터를 이용한 얼굴 인증, 상기 마이크(123)의 입력 음성으로부터 검출된 음성 특징벡터를 이용한 음성 인증, 그리고 상기 입력 영상에 검출된 오브젝트 특징벡터를 이용한 오브젝트 인증을 수행할 수 있다. 그리고 제어부(180)는 얼굴 인증, 음성 인증 및 오브젝트 인증에 따른 모든 결과를 취합하여 상기 사용자에 대한 최종 인증을 수행할 수 있다. 예를 들어, 제어부(180)는 상기 얼굴 인증을 통해 인증된 사용자 얼굴임을 확인하고, 상기 음성 인증을 통해 인증된 사용자 음성임을 확인하고, 상기 오브젝트 인증을 통해 오브젝트의 동작이 이루어진 상태(예컨대, 얼굴의 움직임, 눈의 깜박임, 입의 움직임 등)를 확인할 시 상기 사용자를 인증된 사용자인 것으로 판별할 수 있다.

[0065] 또는 제어부(180)는 상기 카메라 모듈(110)의 입력 영상으로부터 검출된 얼굴 특징벡터를 이용한 얼굴 인증, 상기 마이크(123)의 입력 음성으로부터 검출된 음성 특징벡터를 이용한 음성 인증, 그리고 상기 입력 영상에서 검출된 오브젝트의 특징벡터와 상기 음성 특징벡터에 따른 입술 동작과 음성 간의 동기화 인증을 수행할 수 있다. 그리고 제어부(180)는 얼굴 인증, 음성 인증 및 동기화 인증에 따른 모든 결과를 취합하여 상기 사용자에 대한 최종 인증을 수행할 수 있다. 예를 들어, 제어부(180)는 상기 얼굴 인증을 통해 인증된 사용자 얼굴임을 확인하고, 상기 음성 인증을 통해 인증된 사용자 음성임을 확인하고, 상기 동기화 인증을 통해 발화된 음성과 그에 따른 입술 동작의 일치함을 확인할 시 상기 사용자를 인증된 사용자인 것으로 판별할 수 있다.

[0066] 다음으로, 제어부(180)는 상기와 같은 복합적인 인증에 의해 상기 사용자가 인증된 사용자임을 판별할 시 사용자 인증을 정상 처리하고 인증 모드를 해제할 수 있다. 예를 들어, 제어부(180)는 잠금 기능 해제 및 상기 락스

프린의 표시를 생략하고 참조번호 <511>에 나타낸 바와 같이 실행화면 표시를 제어할 수 있다. 상기 실행화면은 홈스크린이거나 상기 사용자 디바이스(100)가 대기모드(표시부 턴-오프 전입 상태) 이전에 실행된 어플리케이션의 실행화면 등을 나타낼 수 있다.

[0067] 이와 같이, 본 발명의 실시 예에 따르면, 복합 생체인식 정보를 이용한 사용자 인증을 수행하되, 오브젝트 특정 벡터의 동작 상태를 추가 감지하거나, 입술 동작과 입력 음성의 동기화 상태를 추가 감지하는 것에 의해 보다 강화된 사용자 인증을 수행할 수 있다. 이에 따라, 상기 사용자 디바이스(100)를 불법 사용하고자 하는 사용자가 정시 사용자의 사진 및 녹취된 음성으로 사용자 디바이스(100)의 불법 사용을 방지하거나, 사용자 인증이 필요한 다양한 정보로의 접근을 미연에 차단할 수 있다. 그리고 이상에서는 본 발명의 인증 모드가 잠금 기능에 따른 락스크린을 해제하는 예시에 적용되는 것을 설명하였다. 하지만, 본 발명의 실시 예에 따른 상기 인증 모드는 사용자가 타인으로부터 보호하고자 하는 정보(예컨대, 주소록, 개인 데이터 등), 사용자 디바이스(100)를 이용한 금융 서비스 접근의 허용 여부 판별, 그리고 사용자 디바이스(100)에서 과금이 발생하는 서비스 등에 대해서도 인증 모드를 설정하고, 앞서와 같은 사용자 통합 인증을 수행할 수 있다.

[0068] 도 6은 본 발명의 실시 예에 따른 사용자 디바이스(100)에서 사용자 인증을 위한 통계모델 등록 방법을 도시한 흐름도이다.

[0069] 상기 도 6을 참조하면, 제어부(180)는 사용자 요청에 응답하여 인증 설정 모드 진입(601단계) 시 인증 관련 구성을 구동할 수 있다(603단계). 상기 인증 관련 구성은 복합 생체인식 정보 인식을 위한 구성을 나타내며, 본 발명에서는 카메라 모듈(110) 및 마이크(123)를 포함할 수 있다. 여기서, 상기 도 6에서는 생략하였으나, 상기 인증 설정 모드 진입 시 인증 모드를 수행하고자 하는 카테고리(category)를 선택할 수 있는 사용자 인터페이스(UI, User Interface)가 제공될 수 있다. 예를 들어, 잠금 기능 해제 시 인증 모드 실행, 주소록 진입 시 인증 모드 실행, 금융 서비스 진입 시 인증 모드 실행, 과금 서비스 진입 시 인증 모드 실행 등과 같은 다양한 카테고리에 대한 인증 모드를 설정할 수 있다. 그리고 상기 사용자 인터페이스를 통해 하나 또는 그 이상의 카테고리의 설정이 완료될 시 상기 인증 관련 구성 구동될 수 있도록 구현될 수 있다.

[0070] 다음으로, 제어부(180)는 상기 인증 관련 구성(특히, 카메라 모듈(110) 및 마이크(123))이 구동되면, 상기 카메라 모듈(110)을 통해 전달되는 얼굴 영상을 획득하고(605단계) 상기 마이크(123)를 통해 전달되는 음성을 획득할 수 있다(607단계). 즉, 본 발명에서 사용자 인증을 위한 통계모델은 크게 얼굴 학습 과정과 음성 학습 과정으로 구분되고, 상기 얼굴 학습 과정과 상기 음성 학습 과정을 통해 얼굴 인식용 통계모델과 음성 인식용 통계모델을 구성할 수 있다. 이때, 상기 얼굴 학습 과정과 음성 학습 과정은 동시 진행되거나 또는 계별(시계열) 진행될 수 있으며, 상기 도 6에서는 병렬적으로 동시 진행되는 처리 동작을 예시로 나타낸다. 상기 각 학습 과정들의 병렬 또는 시계열 운용 방식은 사용자 설정에 따라 결정될 수 있다.

[0071] 상기 얼굴 학습 과정에 따르면, 제어부(180)는 상기 획득된 얼굴 영상으로부터 얼굴을 추출하고(611단계), 추출된 얼굴로부터 얼굴 특징벡터를 검출할 수 있다(613단계). 예를 들어, 제어부(180)는 상기 카메라 모듈(110)을 통해 입력되는 얼굴 영상으로부터 얼굴 영역, 눈 영역, 그리고 입 영역 등의 특징을 구분하여 얼굴을 추출할 수 있다. 그리고 제어부(180)는 추출된 얼굴의 특징 중 눈의 중심점 등을 이용하여 얼굴 형상에 대한 정규화를 수행하고, 정규화된 얼굴 영상에서 얼굴 특징벡터를 검출할 수 있다. 다음으로, 제어부(180)는 상기 얼굴 특징벡터를 이용한 얼굴 인증 학습(615단계)을 통해 얼굴 인식용 통계모델을 생성하여(617단계) 저장부(140)의 해당 영역(예컨대, 얼굴정보 저장영역(160))에 저장할 수 있다(619단계). 예를 들어, 제어부(180)는 SVM(Support Vector Machine)과 같은 기계 학습 알고리즘(machine learning algorithm)을 기반으로 상기 얼굴 특징벡터에 대한 학습을 수행하여 사용자 얼굴 인증을 위한 판별 기준인 얼굴 인식용 통계모델을 구축할 수 있다.

[0072] 상기 음성 학습 과정에 따르면, 상기 제어부(180)는 상기 획득된 음성으로부터 음성 특징벡터를 검출할 수 있다(621단계). 예를 들어, 제어부(180)는 상기 마이크(123)를 통해 입력되는 음성으로부터 톤, 주파수, 어휘, 속도 등의 특징을 분석하여 음성 특징벡터를 검출할 수 있다. 그리고 제어부(180)는 상기 음성 특징벡터를 이용한 음성 인증 학습(623단계)을 통해 음성 인식용 통계모델을 생성하여(625단계) 저장부(140)의 해당 영역(예컨대, 음성정보 저장영역(170))에 저장할 수 있다(627단계). 예를 들어, 제어부(180)는 앞서와 같이 SVM과 같은 기계 학습 알고리즘을 기반으로 상기 음성 특징벡터에 대한 학습을 수행하여 사용자 음성 인증을 위한 판별 기준인 음성 인식용 통계모델을 구축할 수 있다.

[0073] 한편, 상기 도 6에서는 생략하였으나, 사용자는 인증 모드의 운용 방식에 대한 설정을 추가적으로 행할 수 있다. 예를 들어, 앞서 도 2를 참조한 설명과 같이 얼굴 인증, 음성 인증 및 오브젝트 동작 변화 인증을 기반으로 하는 통합 인증 방식과, 앞서 도 3을 참조한 설명과 같이 얼굴 인증, 음성 인증 및 동기화 인증(입술 오브젝

트의 동작 변화와 입력 음성 간의 동기화 여부)을 기반으로 하는 통합 인증 방식 중 어느 하나의 방식을 설정할 수 있다. 이때, 전자의 통합 인증 방식의 경우 동작 변화를 인증하고자 하는 오브젝트 타입(예컨대, 얼굴의 움직임, 눈의 깜박임, 입의 움직임 등)을 추가적으로 설정할 수도 있다.

[0074] 도 7은 본 발명의 실시 예에 따른 사용자 디바이스(100)에서 사용자 인증 방법을 도시한 흐름도이다.

[0075] 상기 도 7을 참조하면, 제어부(180)는 사용자 디바이스(100)의 특정 기능 실행에 응답하여 인증 모드 진입(701단계) 시 인증 관련 구성을 구동할 수 있다(703단계). 예를 들어, 제어부(180)는 사용자의 특정 기능 실행이 요청될 시, 상기 기능 실행에 사용자 인증을 위한 인증 모드가 설정되어 있는지 여부를 판별할 수 있다. 상기 기능 실행에 인증 모드가 설정된 경우 상기 인증 모드 진입을 제어할 수 있다. 그리고 제어부(180)는 상기 인증 모드 진입 시 사용자 인증을 위해 설정된 카메라 모듈(110)과 마이크(123)를 구동할 수 있다. 상기 인증 모드가 설정되는 기능은 앞서 살펴본 바와 같이, 잠금 기능, 금융 서비스, 과금 서비스, 주소록 등 사용자 설정에 따른 기능일 수 있다.

[0076] 다음으로, 제어부(180)는 상기 인증 관련 구성이 구동되면, 상기 카메라 모듈(110)을 통해 전달되는 얼굴 영상을 획득하고(705단계) 상기 마이크(123)를 통해 전달되는 음성을 획득할 수 있다(707단계). 본 발명에서 사용자 인증을 위한 인증 과정은 크게 영상 인증 과정과 음성 인증 과정으로 구분되고, 상기 영상 인증 과정과 상기 음성 인증 과정은 병렬적 또는 시계열적으로 운용할 수 있다. 그리고 상기 영상 인증 과정은 크게 얼굴 인증 과정과 오브젝트 인증 과정으로 구분될 수 있으며, 얼굴 인증 과정 및 오브젝트 인증 과정은 병렬적 또는 시계열적으로 운용할 수 있다. 상기 각 인증 과정들의 병렬 또는 시계열 운용 방식은 사용자 설정에 의해 결정될 수 있다.

[0077] 상기 영상 인증 과정 중 얼굴 인증 과정에 따르면, 제어부(180)는 상기 획득된 얼굴 영상으로부터 얼굴을 추출하고(711단계), 추출된 얼굴로부터 얼굴 특징벡터를 검출할 수 있다(713단계). 예를 들어, 제어부(180)는 상기 카메라 모듈(110)을 통해 입력되는 얼굴 영상으로부터 얼굴 영역, 눈 영역, 그리고 입 영역 등의 특징을 구분하여 얼굴을 추출할 수 있다. 그리고 제어부(180)는 추출된 얼굴의 특징 중 눈의 중심점 등을 이용하여 얼굴 형상에 대한 정규화를 수행하고, 정규화된 얼굴 영상에서 얼굴 특징벡터를 검출할 수 있다. 다음으로, 제어부(180)는 상기 얼굴 특징벡터와 학습된 얼굴 인식용 통계모델을 비교하는 것에 의해 얼굴 인증을 수행하고(715단계), 그에 따른 얼굴 인증정보를 생성할 수 있다(717단계).

[0078] 상기 영상 인증 과정 중 오브젝트 인증 과정에 따르면, 제어부(180)는 상기 획득된 얼굴 영상으로부터 오브젝트를 검출하고(721단계), 검출된 오브젝트로부터 오브젝트 특징벡터를 검출할 수 있다(723단계). 상기 오브젝트는 사용자의 얼굴에서 움직임을 판별하기 위한 요소로, 상기 도 7에서는 얼굴, 눈, 입 등에 해당할 수 있다. 예를 들어, 제어부(180)는 상기 카메라 모듈(110)을 통해 입력되는 얼굴 영상으로부터 얼굴 영역, 눈 영역, 그리고 입 영역 중 설정된 오브젝트의 위치를 검출하고, 검출된 오브젝트의 위치에서 상기 오브젝트의 동작(움직임)을 나타내는 오브젝트 특징벡터(예컨대, 얼굴의 움직임, 눈의 깜박임, 입의 움직임 등)를 검출할 수 있다. 다음으로, 제어부(180)는 상기 오브젝트 특징벡터로부터 오브젝트의 동작 여부를 판단하고(725단계), 그에 따른 동작정보를 생성할 수 있다(725단계).

[0079] 상기 음성 인증 과정에 따르면, 제어부(180)는 상기 획득된 음성으로부터 음성 특징벡터를 검출할 수 있다(731단계). 예를 들어, 제어부(180)는 마이크(123)를 통해 입력되는 음성으로부터 톤, 주파수, 어휘, 속도 등의 특징을 분석하여 음성 특징벡터를 검출할 수 있다. 그리고 제어부(180)는 상기 음성 특징벡터와 학습된 음성 인식용 통계모델을 비교하는 것에 의해 음성 인증을 수행하고(733단계), 그에 따른 음성 인증정보를 생성할 수 있다(735단계).

[0080] 다음으로, 제어부(180)는 상기 얼굴 인증정보, 동작정보, 그리고 음성 인증정보를 기반으로 통합 인증을 수행하고(741단계), 그에 따른 인증 결과를 출력할 수 있다(743단계). 예를 들어, 제어부(180)는 상기 얼굴 인증정보를 통해 인증된 사용자 얼굴임을 확인하고, 상기 음성 인증정보를 통해 인증된 사용자 음성임을 확인하고, 상기 동작정보를 통해 오브젝트의 동작이 이루어짐을 확인할 시 상기 사용자에 대한 사용자 인증을 정상 처리하고, 그에 따른 인증 결과를 출력(예컨대, 락스크린 해제, 과금 서비스 허용, 주소록 표시 등)할 수 있다. 또는 제어부(180)는 상기 얼굴 인증정보를 통해 비인증된 사용자 얼굴임을 확인하거나, 상기 음성 인증정보를 통해 비인증된 사용자 음성임을 확인하거나, 또는 상기 동작정보를 통해 오브젝트의 동작이 이루어지지 않음을 확인할 시 상기 사용자에 대한 사용자 인증을 에러 처리하고, 그에 따른 인증 결과를 출력(인증 실패에 대응하는 에러 피드백 정보 출력 등)할 수 있다.

[0081] 도 8은 본 발명의 실시 예에 따른 사용자 디바이스(100)에서 사용자 인증 방법을 도시한 흐름도이다.

[0082] 상기 도 8을 참조하면, 제어부(180)는 앞서 설명한 바와 같이 사용자 디바이스(100)의 특정 기능 실행에 응답하여 인증 모드 진입(801단계) 시 카메라 모듈(110) 및 마이크(123)와 같은 인증 관련 구성을 구동할 수 있다(803단계).

[0083] 다음으로, 제어부(180)는 상기 인증 관련 구성이 구동되면, 상기 카메라 모듈(110)을 통해 전달되는 얼굴 영상을 획득하고(805단계) 상기 마이크(123)를 통해 전달되는 음성을 획득할 수 있다(807단계). 본 발명에서 사용자 인증을 위한 인증 과정은 앞서 살펴본 바와 같이 크게 영상 인증 과정과 음성 인증 과정으로 구분되며, 또한 상기 영상 인증 과정은 크게 얼굴 인증 과정과 오브젝트 인증 과정으로 구분될 수 있으며, 이러한 인증 과정들은 그 운용 방식에 따라 병렬적 또는 시계열적으로 이루어질 수 있다.

[0084] 상기 영상 인증 과정 중 얼굴 인증 과정에 따르면, 제어부(180)는 상기 획득된 얼굴 영상으로부터 얼굴을 추출하고(811단계), 추출된 얼굴로부터 얼굴 특징벡터를 검출할 수 있다(813단계). 그리고 제어부(180)는 검출된 얼굴 특징벡터와 학습된 얼굴 인식용 통계모델을 비교하는 것에 의해 사용자에 대한 얼굴 인증을 수행하고(815단계), 그에 따른 얼굴 인증정보를 생성할 수 있다(817단계).

[0085] 상기 영상 인증 과정 중 오브젝트 인증 과정에 따르면, 제어부(180)는 상기 획득된 얼굴 영상으로부터 오브젝트를 검출하고(821단계), 검출된 오브젝트로부터 오브젝트 특징벡터를 검출할 수 있다(823단계). 그리고 제어부(180)는 상기 오브젝트 특징벡터와 상기 음성 인증 과정에서 검출된 음성 특징벡터를 기반으로, 두 특징벡터들 간의 동기화 여부를 체크하고(825단계), 그에 따른 동기화 정보를 생성할 수 있다(827단계). 즉, 제어부(180)는 상기 오브젝트 특징벡터와 상기 음성 특징벡터가 시간적으로 동기화되어 있는지 판별할 수 있다. 예를 들어, 제어부(180)는 상기 오브젝트 특징벡터에 따른 입술의 움직이는 동작과 상기 음성 오브젝트에 따른 음성의 동적 특성을 비교하고, 두 특성이 동기화되어 있는지 여부를 판별할 수 있다. 그리고 제어부(180)는 동기화 여부 판별에 따른 동기화 정보를 생성할 수 있다.

[0086] 상기 음성 인증 과정에 따르면, 제어부(180)는 상기 획득된 음성으로부터 음성 특징벡터를 검출할 수 있다(831단계). 그리고 제어부(180)는 검출된 음성 특징벡터와 학습된 음성 인식용 통계모델을 비교하는 것에 의해 사용자에 대한 음성 인증을 수행하고(833단계), 그에 따른 음성 인증정보를 생성할 수 있다. 여기서, 제어부(180)는 앞서 설명한 바와 같이 검출된 음성 특징벡터를 이용하여 음성 인증을 수행하면서, 상기 음성 특징벡터의 상기 오브젝트 특징벡터 간의 동기화 인증을 수행할 수 있다.

[0087] 다음으로, 제어부(180)는 상기 얼굴 인증정보, 동기화 정보, 그리고 음성 인증정보를 기반으로 통합 인증을 수행하고(841단계), 그에 따른 인증 결과를 출력할 수 있다(843단계). 예를 들어, 제어부(180)는 상기 얼굴 인증정보를 통해 인증된 사용자 얼굴임을 확인하고, 상기 음성 인증정보를 통해 인증된 사용자 음성임을 확인하고, 상기 동기화 정보를 통해 오브젝트 특징벡터와 음성 특징벡터 간의 동기화가 일치하는 것을 확인할 시 상기 사용자에 대한 인증을 정상 처리하고, 그에 따른 인증 결과를 출력할 수 있다. 또는 제어부(180)는 상기 얼굴 인증정보를 통해 비인증된 사용자 얼굴임을 확인하거나, 상기 음성 인증정보를 통해 비인증된 사용자 음성임을 확인하거나, 또는 상기 동기화 정보를 통해 오브젝트 특징벡터와 음성 특징벡터 간의 동기화가 일치하지 않는 것을 확인할 시 상기 사용자에 대한 사용자 인증을 에러 처리하고, 그에 따른 인증 결과를 출력할 수 있다.

[0088] 도 9는 본 발명의 실시 예에 따른 사용자 디바이스(100)에서 사용자 인증을 위한 운용 방법을 도시한 흐름도이다.

[0089] 특히, 상기 도 9에서는 카메라 모듈(110) 및 마이크(123) 중 어느 하나로부터 일 생체인식 정보가 제공되고, 다른 하나로부터 타 생체인식 정보가 제공되지 않은 경우, 그에 대한 에러 또는 유효 여부를 결정하는 동작을 나타낸 것이다.

[0090] 상기 도 9를 참조하면, 제어부(180)는 앞서 설명한 바와 같이 사용자 디바이스(100)의 특정 기능 실행에 응답하여 인증 모드 진입(901단계) 시 카메라 모듈(110) 및 마이크(123)와 같은 인증 관련 구성을 구동할 수 있다(903단계).

[0091] 제어부(180)는 상기 인증 관련 구성이 구동되면, 상기 카메라 모듈(110) 및 마이크(123)로부터 적어도 하나의 생체인식 정보가 검출되는지 판단할 수 있다(905단계).

[0092] 제어부(180)는 상기 카메라 모듈(110) 및 마이크(123)로부터 어떠한 생체인식 정보도 검출되지 않을 시(905단계의 NO) 사용자 인증 에러로 판정하고(919단계), 그에 따른 에러 피드백 정보 출력을 제어할 수 있다(921단계).

이는, 상기 카메라 모듈(110)을 통해 사용자의 얼굴이 입력되지 않고, 상기 마이크(123)를 통해 사용자의 음성이 입력되지 않은 상태일 수 있다. 이때, 상기 도 9에서는 생략하였으나, 제어부(180)는 상기 에러 판정 시 미리 설정된 설정시간동안 생체인식 정보 검출을 대기한 후, 상기 설정시간 경과 시까지 생체인식 정보가 검출되지 않을 시 에러로 결정할 수 있다.

[0093] 제어부(180)는 상기 카메라 모듈(110) 및 마이크(123)로부터 적어도 하나의 생체인식 정보가 검출될 시(905단계의 YES) 상기 검출된 생체인식 정보가 복수에 해당하는 복합 생체인식 정보인지 판단할 수 있다(907단계). 그리고 제어부(180)는 상기 복합 생체인식 정보인 것으로 판단할 시(907단계의 YES) 앞서 살펴본 바와 같은 절차에 따라 상기 복합 생체인식 정보를 이용한 통합 인증을 수행할 수 있다(909단계). 반면, 제어부(180)는 하나의 생체인식 정보인 것으로 판단할 시(907단계의 NO) 상기 생체인식 정보가 음성 인식정보에 해당하는지 영상 인식정보에 해당하는지 판단할 수 있다(911단계).

[0094] 제어부(180)는 상기 911단계에서 음성 인식정보인 것으로 판단할 시(911단계의 YES), 상기 마이크(123)를 통해 입력된 음성을 이용하여 앞서 살펴본 바와 같은 절차에 따라 음성 인증을 수행하면서, 상기 카메라 모듈(110)에 의한 영상 획득을 대기할 수 있다(913단계). 그리고 제어부(180)는 영상 획득 대기 중에 영상 획득 여부를 체크할 수 있다(915단계).

[0095] 제어부(180)는 영상이 획득되면(915단계의 YES), 상기 사용자에 대한 통합 인증을 수행할 수 있다(909단계). 이때, 제어부(180)는 상기 카메라 모듈(1110)을 통해 입력된 영상을 이용한 영상 인증을 수행한 후, 상기 음성 인증에 따른 음성 인증정보와 상기 영상 인증에 따른 영상 인증정보를 기반으로 하는 통합 인증을 수행할 수 있다.

[0096] 제어부(180)는 영상이 획득되지 않으면(915단계의 NO), 상기 마이크(123)를 통한 음성 입력이 종료되는지 여부를 판별할 수 있다(917단계). 제어부(180)는 음성 입력이 종료되지 않으면(917단계의 NO) 상기 913단계로 진행하여 이하의 동작을 수행할 수 있다. 제어부(180)는 음성 입력이 종료되면(917단계의 YES) 사용자 인증 에러로 판정하고(919단계), 그에 따른 에러 피드백 정보 출력을 제어할 수 있다(921단계).

[0097] 제어부(180)는 상기 911단계에서 영상 인식정보인 것으로 판단할 시(911단계의 NO), 상기 카메라 모듈(110)을 통해 입력된 영상을 이용하여 앞서 살펴본 바와 같은 절차에 따라 영상 인증을 수행하면서, 상기 마이크(123)에 의한 음성 획득을 대기할 수 있다(923단계). 그리고 제어부(180)는 음성 획득 대기 중에 음성 획득 여부를 체크할 수 있다(925단계).

[0098] 제어부(180)는 음성이 획득되면(925단계의 YES), 상기 사용자에 대한 통합 인증을 수행할 수 있다(929단계). 이때, 제어부(180)는 상기 마이크(123)를 통해 입력된 음성을 이용한 음성 인증을 수행한 후, 상기 영상 인증에 따른 영상 인증정보와 상기 음성 인증에 따른 음성 인증정보를 기반으로 하는 통합 인증을 수행할 수 있다.

[0099] 제어부(180)는 음성이 획득되지 않으면(925단계의 NO), 미리 정의된 설정시간이 경과되는지 여부를 판별할 수 있다(927단계). 제어부(180)는 설정시간이 경과되지 않으면(927단계의 NO) 상기 923단계로 진행하여 이하의 동작을 수행할 수 있다. 제어부(180)는 설정시간이 경과되면(927단계의 YES) 사용자 인증 에러로 판정하고(919단계), 그에 따른 에러 피드백 정보 출력을 제어할 수 있다(921단계).

[0100] 한편, 사용자는 사용자 디바이스(100)를 이용한 사용자가 사용자 인증 시, 음성 인증을 위한 발화 시 여러 가지 이유로 마이크(123)를 사용자 입 주위로 위치시키는 행위를 할 수 있다. 예를 들어, 타인으로부터 발화하는 음성의 누출을 방지하거나 또는 조용한 환경에서 조용히 발화를 해야 하는 상황에서, 사용자는 마이크(123)를 사용자 입에 인접하여 발화할 수 있다. 이러한 경우, 카메라 모듈(110)에 의해서는 사용자 얼굴이 인식되지 않은 상태일 수 있다. 또는 사용자는 사용자 얼굴을 먼저 인식 시킨 후 음성 입력을 위한 발화를 시간차를 두고 입력할 수도 있다. 따라서 본 발명에서는 위와 같은 다양한 환경을 고려하여, 각각의 생체인식 정보가 동시에 인식되지 않고 어느 하나의 생체인식 정보만 인식되는 경우에도, 설정된 루틴에 따라 인식되지 않은 생체인식 정보의 입력을 일정 범위만큼 대기하는 것을 통해 사용자 의도와는 무관하게 이루어지는 무분별한 에러 판정을 줄일 수 있도록 한다.

[0101] 한편, 상술한 바와 같은 본 발명의 사용자 디바이스에서 복합 생체인식 정보를 이용한 사용자 인증 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터로 판독 가능한 기록 매체에 기록될 수 있다. 이때, 상기 컴퓨터로 판독 가능한 기록 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 한편, 기록 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다.

[0102] 상기 컴퓨터로 판독 가능한 기록 매체에는 하드디스크, 플로피디스크 및 자기 테이프와 같은 자기매체(Magnetic Media), CD-ROM(Compact Disc Read Only Memory), DVD(Digital Versatile Disc)와 같은 광기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-Optical Media), 및 ROM(Read Only Memory), RAM(Random Access Memory), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 또한 프로그램 명령에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드 뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상술한 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0103] 그리고 본 명세서와 도면에 개시된 본 발명의 실시 예들은 본 발명의 기술 내용을 쉽게 설명하고 본 발명의 이해를 돕기 위해 특정 예를 제시한 것일 뿐이며, 본 발명의 범위를 한정하고자 하는 것은 아니다. 따라서 본 발명의 범위는 여기에 개시된 실시 예들 이외에도 본 발명의 기술적 사상을 바탕으로 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

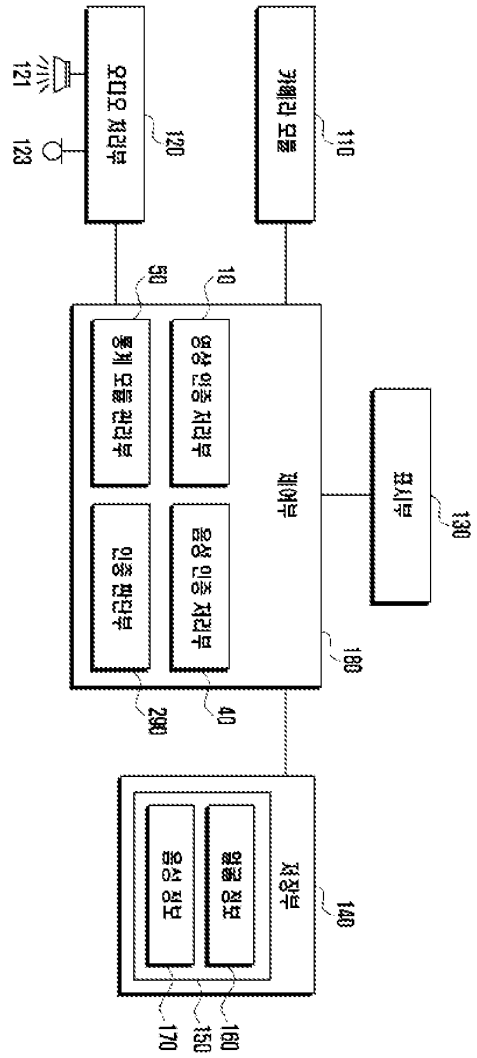
부호의 설명

[0104] 100: 사용자 디바이스

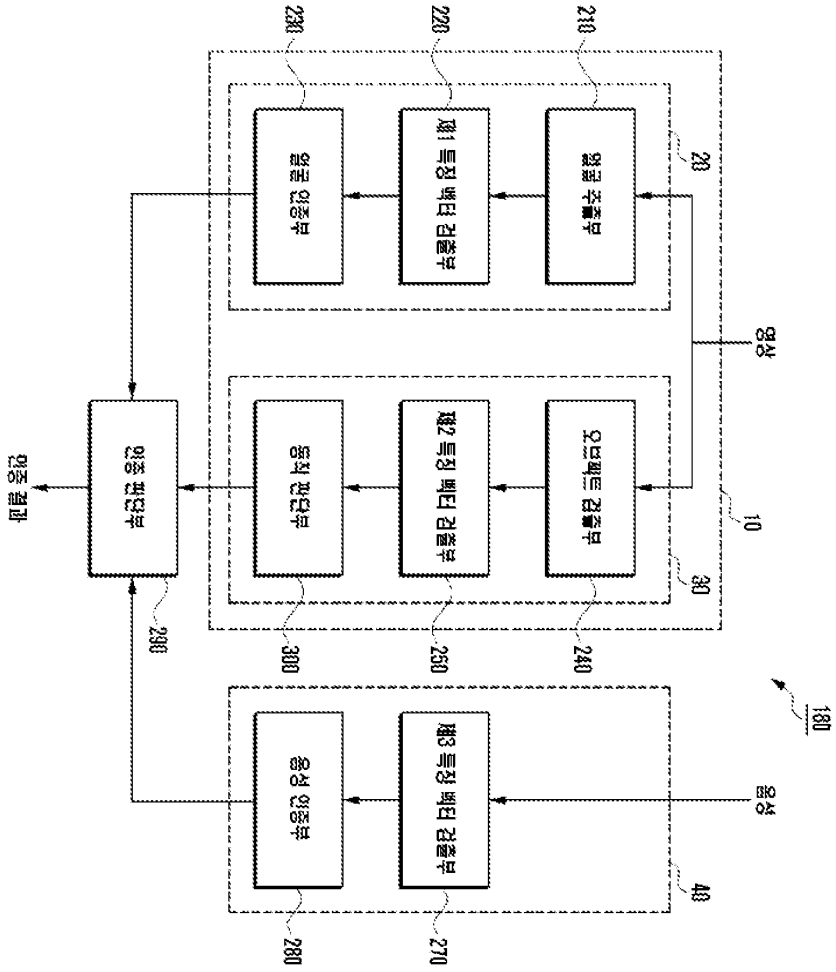
110: 카메라 모듈	120: 오디오처리부
121: 스피커	123: 마이크
130: 표시부	140: 저장부
150: 학습정보 저장영역	160: 얼굴정보 저장영역
170: 음성정보 저장영역	180: 제어부
10: 영상 인증 처리부	40: 음성 인증 처리부
50: 통계모델 관리부	200: 동작 판단부
250: 인증 판단부	300: 동기화 판단부

도면

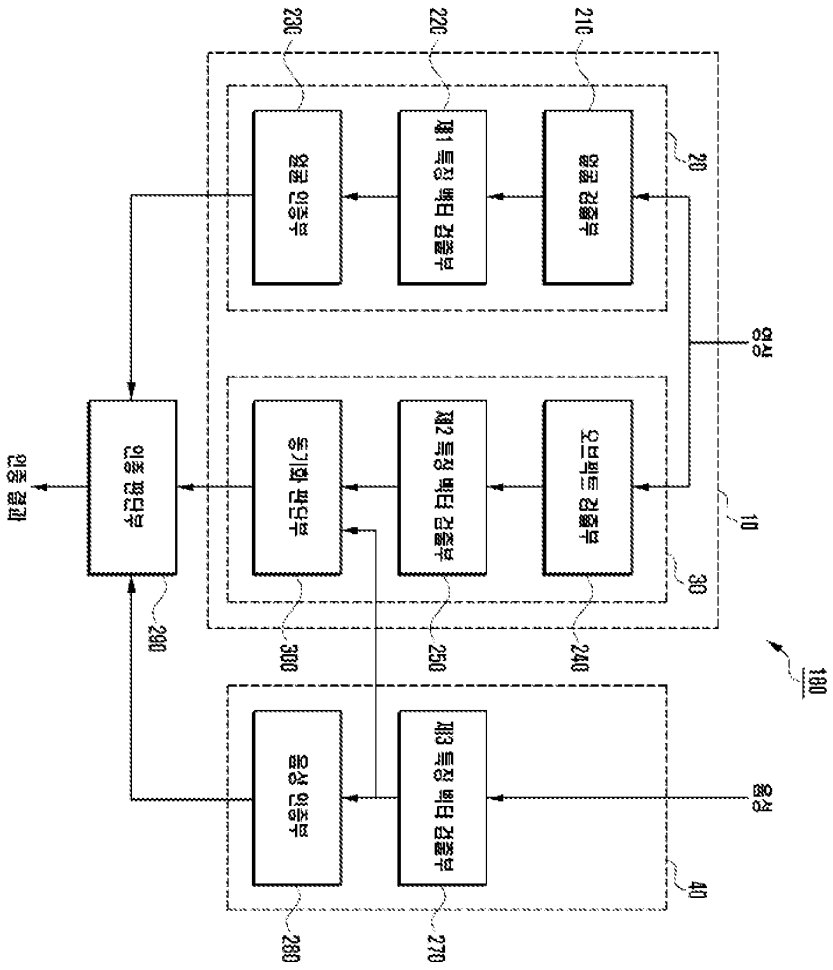
도면1


121
123
오디오 처리부
120
카메라 모듈
110
50
10
통계 모듈 관리부
영상 인증 처리부
인증 판단부
음성 인증 처리부
제어부
180
표시부
130
200
40
저장부
140
음성 정보
얼굴 정보
170
150
160

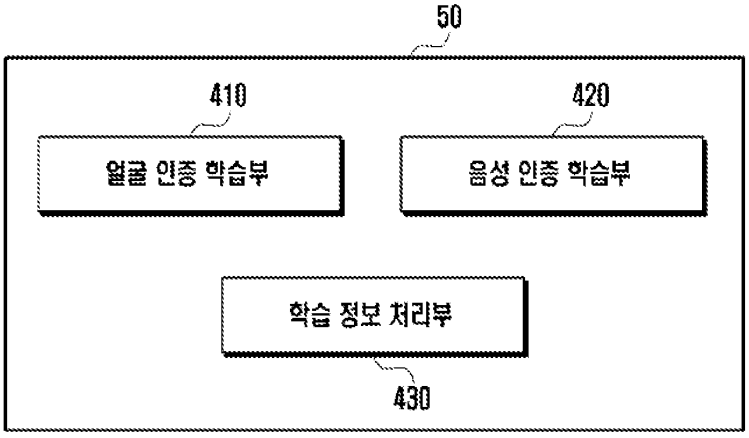
도면2



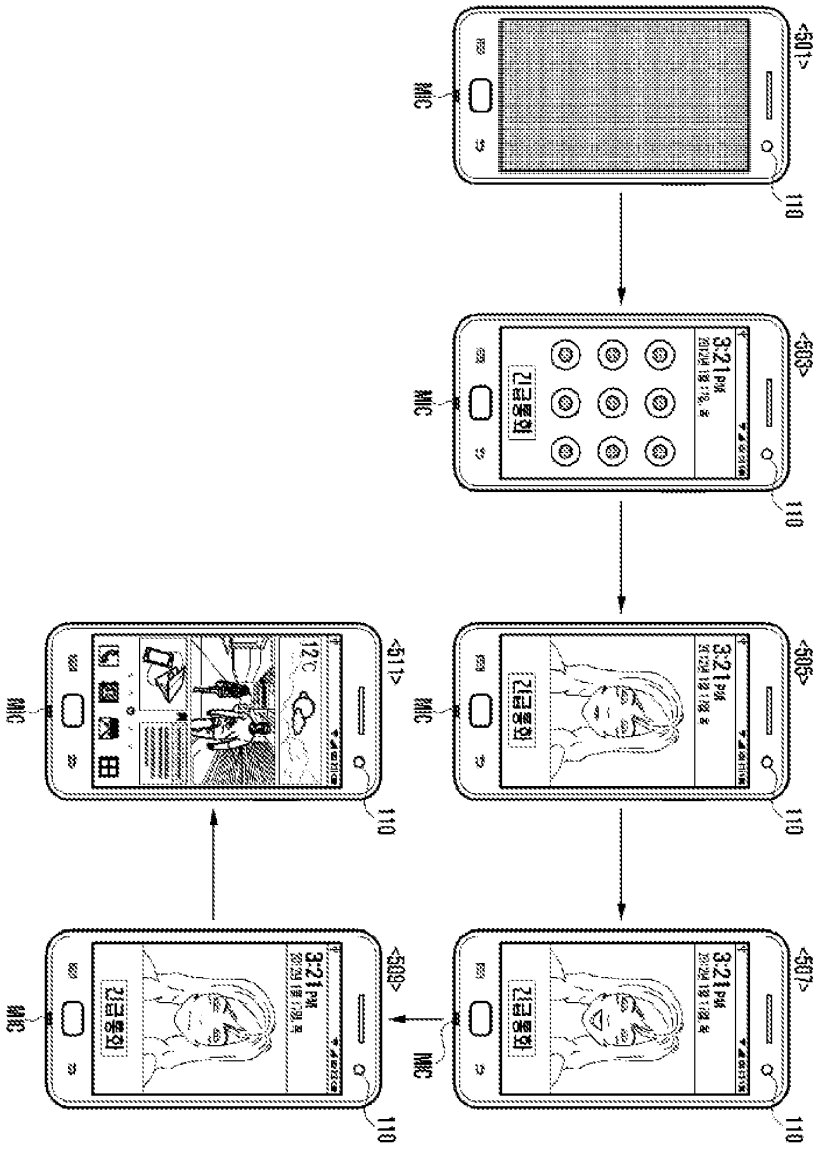
도면3


230
220
210
얼굴 인증부
제1 특징 벡터 검출부
얼굴 검출부
20
영상
인증 결과
인증 판단부
음기화 판단부
제2 특징 벡터 검출부
오브젝트 검출부
10
30
290
300
250
240
180
음성 인증부
제3 특징 벡터 검출부
음성
40
280
270

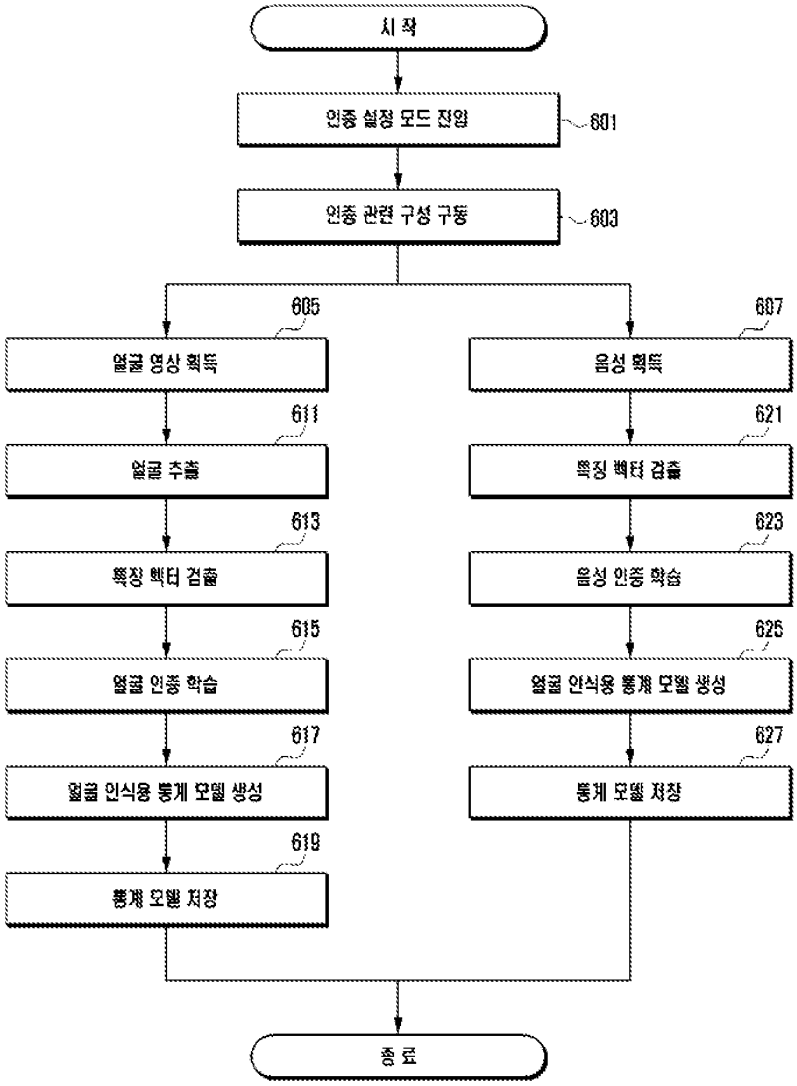
도면4


50
410
420
얼굴 인증 학습부
음성 인증 학습부
학습 정보 처리부
430

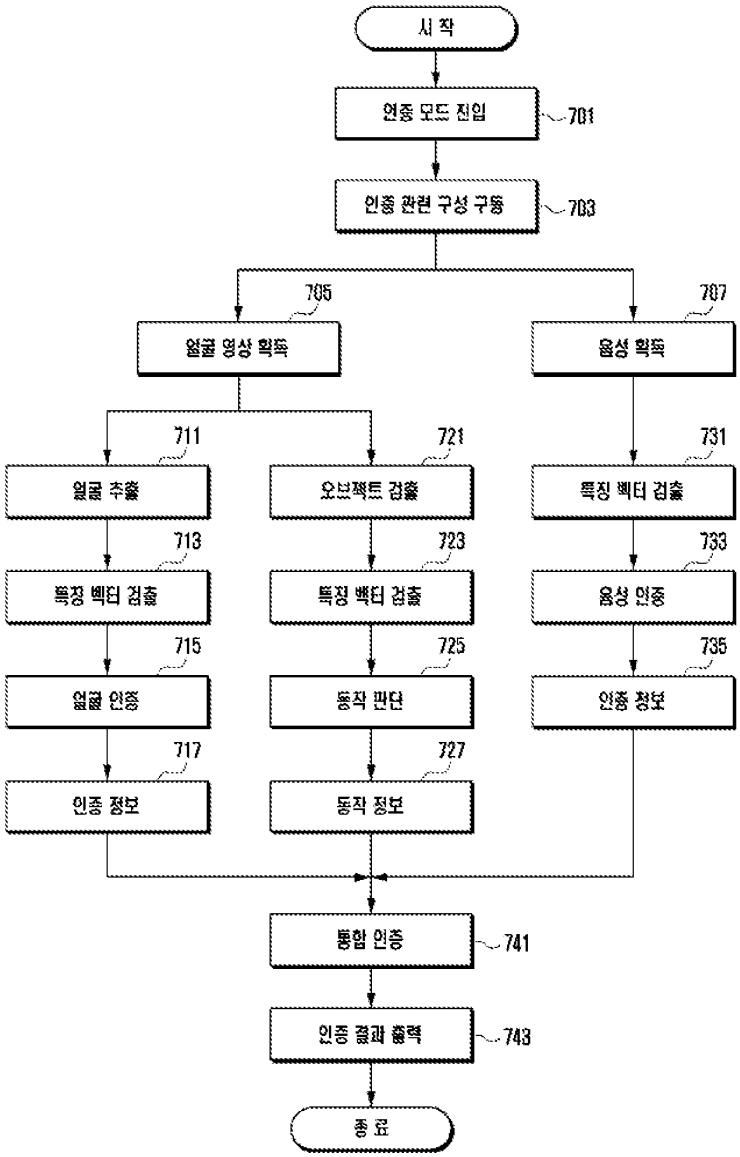
도면5



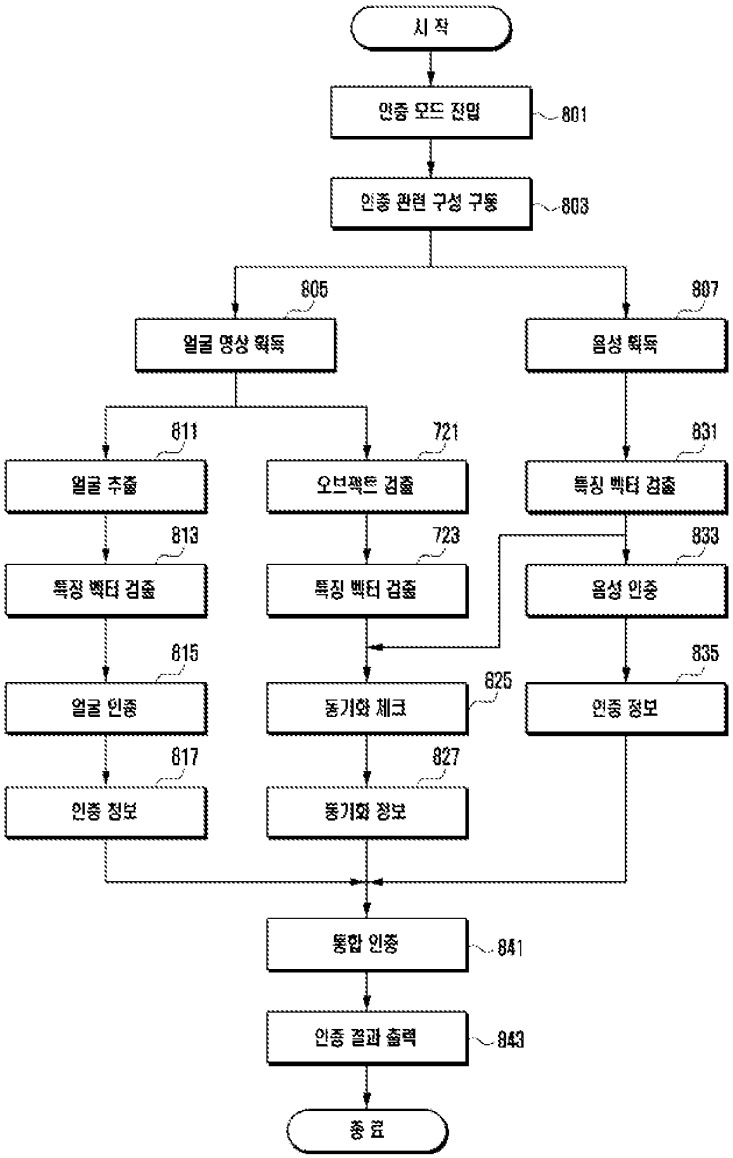
도면6


시작
인증 설정 모드 진입
601
인증 관련 구성 구동
603
605
얼굴 영상 획득
611
얼굴 추출
613
특징 벡터 검출
615
얼굴 인증 학습
617
얼굴 인식용 통계 모델 생성
619
통계 모델 저장
607
음성 획득
621
특징 벡터 검출
623
음성 인증 학습
625
얼굴 인식용 통계 모델 생성
627
통계 모델 저장
종료

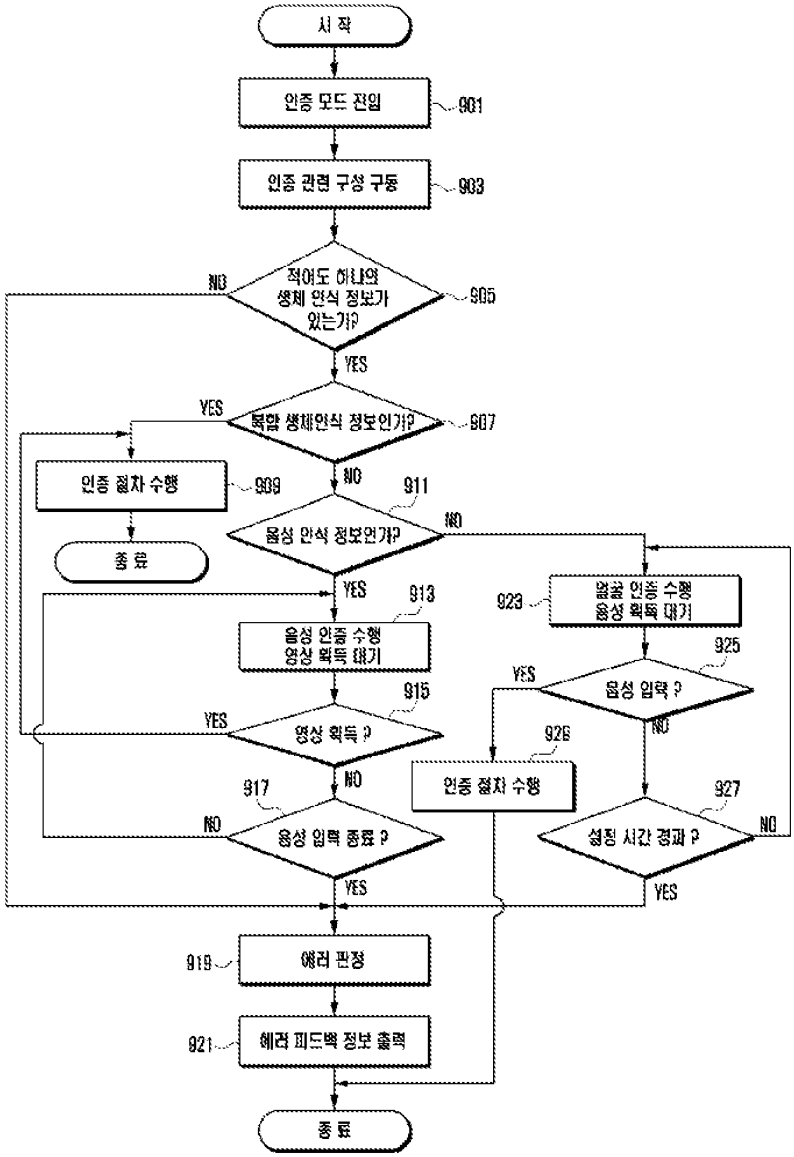
도면7


시작
인증 모드 진입
701
인증 관련 구성 구동
703
705
얼굴 영상 획득
707
음성 획득
711
얼굴 추출
721
오브젝트 검출
731
특징 벡터 검출
713
특징 벡터 검출
723
특징 벡터 검출
733
음성 인증
715
얼굴 인증
725
동작 판단
735
인증 정보
717
인증 정보
727
동작 정보
통합 인증
741
인증 결과 출력
743
종료

도면8


시작
인증 모드 진입
801
인증 관련 구성 구동
803
805
얼굴 영상 획득
807
음성 획득
811
얼굴 추출
721
오브젝트 검출
831
특징 벡터 검출
813
특징 벡터 검출
723
특징 벡터 검출
833
음성 인증
815
얼굴 인증
825
동기화 체크
835
인증 정보
817
인증 정보
827
동기화 정보
통합 인증
841
인증 결과 출력
843
종료

도면9


시 작
인증 모드 진입
901
인증 관련 구성 구동
903
적어도 하나의 생체 인식 정보가 있는가?
905
NO
YES
복합 생체인식 정보인가?
907
YES
인증 절차 수행
909
NO
911
음성 인식 정보인가?
NO
종 료
YES
913
음성 인증 수행 영상 획득 대기
923
얼굴 인증 수행 음성 획득 대기
925
음성 입력 ?
YES
NO
915
영상 획득 ?
YES
926
인증 절차 수행
NO
917
927
음성 입력 종료 ?
NO
설정 시간 경과 ?
NO
YES
YES
919
에러 판정
921
에러 피드백 정보 출력
종 료

Espacenet

Bibliographic data: CN103593594 (A) — 2014-02-19

System and method for providing secure access to an electronic device using facial biometric identification and screen gesture

Inventor(s):	CYRUS AZAR; GEORGE BROSTOFF ± (CYRUS AZAR, ; GEORGE BROSTOFF)
Applicant(s):	SENSIBLE VISION INC ± (SENSIBLE VISION, INC)
Classification:	**- international:** ***G06F21/31; G06F21/32*** **- cooperative:** **G06F21/32**; **G06K9/00221**; **G06K9/00892**; more
Application number:	CN2013108147 20130109
Priority number (s):	US201261584492P 20120109
Also published as:	US2013223696 (A1)

Abstract of CN103593594 (A)

A system and method for providing secure authorization to a device (800) that includes the steps of combining two or more security factors for authentication (805,807) operating at about the same time where at least one of the factors is a "tolerant" factor. By combining two factors analyzed at about the same time (805,807), the tolerance match required by the tolerant factor(s) can be reduced without reducing the overall security accuracy.

Patent Translate
Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

DESCRIPTION CN103593594

A system and method for providing secure authentication to a device (800), comprising: two or more of a safety factor in combination with about the same time for the authentication operation in step (805,807), wherein the at least one factor is "tolerance" factor. About the same time by two factors will be analyzed in combination (805,807), can be reduced tolerance matching tolerance factor required, without reducing the overall safety accuracy.

Systems and methods for using biometric facial recognition and on-screen gestures to provide secure access to electronic device

This patent application claims priority to provisional patent application serial on January 9, 2012 Submitted No. 61 / 584,492 and priority interests, the disclosure of which provisional patent application is incorporated by reference This article.

TECHNICAL FIELD

The present invention relates generally to electronic security, and more particularly relates to the use of screen gestures and facial birth Biometrics to authenticate the user of the electronic apparatus.

Background technique

Many electronic devices (such as personal computers, including mobile phones and personal digital assistants (PDA) Mobile devices) use some form of authentication (usually must be entered into the device's password) to Gain access. Most often, the password is typed into the keyboard or other interface, which then allows Users get access to some or all of the function devices and / or networks. The password associated with the use of Q Problem is that they are time-consuming, and for user input is inconvenient. Users often Use informal password or share their passwords with others, which endanger the security of the system. These ones Negate the value of the actual situation of the password, and makes it difficult to accurately access audit. in addition, Forgotten password management, shared with others or misplaced when it is expensive. Although real Now the use of other types of security access systems, such as voice recognition, fingerprint or iris scan, However, these types of systems require different procedures to access and use the device. To be able to operate, These techniques require specific and time-consuming registration process.

Therefore, the "identity Management" always presents a challenge. Start, the individual has with the user name and password Associated in order to obtain access to the computer system, which results in certification (validation personally, "he They alleged real people ") significant challenge. This usually means that you want to remember and enter for calculating Unique user name and password machine, security applications and multiple sites. The need for additional security control Made systems (for example, online banking), it has been a requirement that individuals using the "two-factor authentication." This You need more than one type of identification, such as a password or PIN plus token. As the user continues to use a plurality of Electronic

equipment and services (for example, smart phones, e-mail, online banking, social networking), remember Record multiple passwords and continue to enter the password has simply become the best-case scenario is not square Then, and for many purposes it is unmanageable situation. Almost every day, news and we are divided Cybercrime enjoy the challenge of how to improve this, ..., forcing the use of a longer, more complex The password, which is a longer, more complex passwords must be frequently changed or risking the loss of important Risk information, privacy, reputation and money. Increased complexity does not encourage strong security measures and policies Little use and comply with these measures and policies. Frustrated users themselves may be faced with security Full risk.

Using face recognition biometric authentication is often used to gain access to the electronic device. Authorize To Kyle and U.S. Patent No.6,853,739 issued to Akiyama et al U.S. Patent No. 6,724,919 (both incorporated by reference herein) discloses the authentication system according to Son, in these authentication system, using the database to the user's facial features and pre-established Database of those features were compared. Once the comparison, and then to carry out inspection certification Card, and unauthorized access to the system. A disadvantage of this type of system is that the user needs single Separate and specific registration process in order to establish a database. On this type of face recognition system And other terms of the prior art systems, the database must be filled prior to use; otherwise, the Department of The system will not operate. This gives the system operator imposes an unnecessary burden on the system needs to be To get training before you can run detailed steps to populate the database. Further, this type of security The system does not allow to automatically update the database to accommodate the position of the head, user characteristics (such as different Glasses) changes the operating characteristics of the camera, lighting and other environmental factors change. This may It limits the database matching (recognition) of speed, precision, and even the success of. Moreover, these now Some facial recognition and other biometric authentication system only at run-time.

Other techniques use gestures and equipment associated display. This type of identification technology involved And touch touchscreen user device and the identified mobile device. These links can move to set up Standby function, such as running certain applications or to allow access to the device. The user's finger gesture Movement of the touch screen, or the shape of the pattern of movement of the user have been identified or selected. some Depending on the exact matching factor, and other factors due to the design of which is used a level of Matching tolerance (also called tolerance factor) to determine the acceptable gesture or certificate. Examples of exact factor Totally including the user's password, smart card or code from a hardware security token. These factors must Before always precise geographical stored certificate match. Tolerance factors include all forms of biometric (Face, voice and fingers), exact match with the stored certificate the existence of a defined deviation / Tolerance is allowed (and the actual work is also needed) patterns and gestures. Even if in some Under some circumstances to accept less than the total length of the password, the password can also become tolerance factor.

Another example of the use of biometric security systems to supplement password entered is licensed to Hwang Etc. U.S. Patent No.7,161,468. The patent describes a user authentication device, based on User-entered password and the user's biometric information to authenticate the user. The user authentication device package Comprising: password input unit that determines whether the password is entered; a storage unit that stores Notes Registered password and biometric registered; threshold setting unit, if you enter a password and registered Password matches, the threshold setting unit sets a first threshold, and if the input password Registered password does not match, then the threshold setting unit sets a second threshold value; and biometric Means configured to obtain biometric information from the outside, determined that the acquired biometric information and the registered Degree of matching biometric information and biometric information, if obtained and registered Biometric information matching degree is greater than the first or the second threshold value, the user authentication is true. As a Within the scope of the present invention is an example of how to adjust such a system, the biometric input can be used to hide Action complement to the rules previously configured and completely user authentication or transfer support secret Code and associated action, such as account constraints fictitious access or warnings are issued.

Finally, Lin U.S. Patent Publication No.2009 / 0160609 describes a lock for the calculation To unlock the device, wherein the user's touch is used to unlock the device request. Biometric information can be used with this process. Although users can use the touch screen to a request for Unlock the device, but Lin did not use a combination of screen gestures and biometric information to authenticate user.

Thus, although in the present art, the use of gestures and a biometric security system is separately available But not currently exist to combine these technologies provide robust security and also to Provide users with a flexible system of access to the electronic device.

BRIEF DESCRIPTION

FIG. 1 is a block diagram illustrating the topology of the system and method of the present invention, wherein a camera Up to the user to provide authentication system.

FIG 2 is a flowchart illustrating an overview of the use of biometric facial method.

Figure 3 is a flowchart illustrating an embodiment of the present invention using an example of a continuous authentication routine.

Figure 4 is a graph showing example after the automatic database used with the timing according to an embodiment of the present invention Flowchart (back-timing) process.

FIG. 5 is a diagram showing facial features according to embodiments of the invention but with the track and delayed locking elements Flowchart routine.

FIG 6 is used in accordance with the present invention, but, in FIG. 5 and the biometric authentication delay lock shown Flow diagram of the embodiment of the replacement routine.

FIG. 7 is a diagram showing the topology of systems and methods according to an alternative embodiment of the invention of the present invention. Block diagram, in which the use of screen gestures and cameras to provide to the user authentication system.

8 is a diagram showing the use of screen gestures and facial biometrics to provide an electronic device certification Another alternative embodiment of a flowchart.

9A and 9B illustrate dynamic gestures to show placement of features touch screen.

FIG. 10 is a diagram showing the use of facial recognition and other factors to authenticate user access to an electronic device stream Chart.

detailed description

Close to the present invention need secure access to all types of electronic equipment for a variety of existing security Full certification exists in the form of basic security vulnerabilities. Existing security method only confirm that the user enters his secret Code, fingerprint or iris scanner time users. The system can not tell whether the current user is a few milliseconds The same individual prior to certification. This makes the device very insecure and vulnerable, until set cancellation Preparation or locked. For malicious people, it takes only a little time you can steal and / Or delete the data the user has logged on the device. Existing programs require the user to manually lock / logout, Or generate user inactivity timer to lock or logoff users.

In addition, most of the information technology (IT) organizations do not want to change because they do not want to take the wind insurance changes, which would affect their existing hardware / software systems. In addition, they do not want to increase the implementation of this A required program support costs. User training and support costs for the help desk to answer questions will It is a big factor. The present invention may be transparent to end users a way to automatically generate the database. this invention requires very little training and very little cost "help desk." Use of the present invention automatic registration Feature, which allows the device to automatically update the database to continuously improve the quality of user identification. In contrast, the current Biometric product requires a specific set of steps to create and update the database. In some cases, only After the initial study, these steps may be performed by the user. In many cases, the system manipulation Before use, IT managers must work together with the user to actually training database.

Compliance with safety is an important issue when it away from your computer, usually require the user to manually Lock or log off their computers. This process is time-consuming, and does not regard the use of calculation Machine during user object is secondary. In addition, the locking or cancellation so that when the user returns provided Standby When you enter a password, which is not great aspect. Unless strict implementation, users often ignore the positive The correct safety procedures. In the

absence of direct supervision under, for system administrators, do not essentially Whether the user is recognized correctly comply with the specified security policy.

An unrealistic scenario typically involves the use of a timer. When a predetermined period of time there is no external Working to make a timer set by the locking device activity. As one skilled in the art know, Peripherals may include, but is not limited to a mouse, keyboard or touch screen. If the timer is set sufficiently Short duration to properly close security holes when the user leaves the device, the device will be in the user Locked data on the viewing screen. Shampoo or cancellation locked each time a user, the user needs to continue Enter their credentials. This results in user-generated frustration, and greatly reduce productivity. Thus, in general Inactive for at least 2-5 minutes, which provides a great vulnerable window. Furthermore, not live Fixed timer is invalid. All Unauthorized users must access the system within the timer period. here Thereafter, an unauthorized user can continue to work indefinitely.

System and method of the present invention to solve such compliance issues directly through automatic processing, thereby ensuring Fully compliant. Because the process is automatic and transparent to the operator, user acceptance is very high. Users find after installing the inventive system easier to use. In addition, it shows a person access device The system audit log is now accurate because this continuous security authentication process. The present invention When the user immediately locked out of sight device / logout, then reappear in the user computer When unlocked to operate as soon as possible before.

Referring now to Figure 1, the system according to the present invention is used as the electronic device 100 comprises 101, which comprises But not limited to personal computers, mobile phones, alphabetically paging devices, personal digital assistants (PDA), video game equipment, etc., which require some type of authentication to gain device 101 Use access. Camera device 105 may also be used to add additional security level, wherein said The camera equipment used in conjunction with the device 101 using a plurality of image vectors to construct an internal database 107. Cameras basically provide real-time images and are generally at a rate of about 5-10 frames per second operation, So that a continuous supply of digital image data to the electronic device 101. And usually makes the camera usually within the apparatus Used in conjunction with optical facial feature tracking software, which is used when the device is located in front of the camera Location tracking surface movement of the user's face. Thus, when the user uses the device, the front of his head After moving around, the software used in conjunction with the camera will track the face movement to allow continuous certification, While using lower CPU and device resources 113.

Those skilled in the art will recognize, the camera 105 may be integrated into the electronic device 101, or Those which can be used as stand-alone accessory or peripheral, for over a wired or wireless connection to transmit image data To the electronic device. A preferred method of the present invention, as described, the microprocessor 109 and comparator 111 together make Used to determine whether the image camera 105 is supplied continuously face image. If it detects a human face Those images image, you can determine whether the image is stored in the user database during the previous 107 In a match to any image. Each vector represents 105 sent from the camera to a digital electronic device 101 Numerical representation of the image. As discussed herein, the electronic device 101 to establish a database Vector 107 The amount of the current vector and the camera 105 is provided for comparison. When it is determined with certainty match and the user is Authentication, the system 100 can be configured to allow a user to access restricted or completely electronic device 101.

FIG. 2 is a diagram showing the overall flow face 100 according to an embodiment of the present invention is a method of biometric Chart. Although this method is shown in the sequence described in 2, but the skilled artisan, Without departing from the spirit and scope of the present method, the reuse and other definitions are possible, which is Obvious. These methods may include two-dimensional (2D), three-dimensional (3D) Infrared (IR) And / or other facial recognition technology, but not limited thereto. In the face biometric for 200 square outlined Method, in 201 starts for the initial start-up logon process equipment, equipment display screen 203, thereby it allows users to provide their login password or other authentication credentials. At 205, associated with the device from the imaging Head receiving video frame, wherein 207, by using face detection, the use of the device determines from the camera Whether the received image data is a face image. If it is not the facial image, the device continues to wait User login credentials (203).

However, if the image data is a face image, then start the timer to remind the user (209). The timer is used to remind the user to determine whether a predetermined time, wherein at the time, the user should User display a message requesting the user to manually enter their credentials before being certified. User alerts timer Expires, unlike recommend the user to manually login,

no certification influential, because the certification process has exceeded Over the expected duration, and the system will benefit from database updates. Therefore, even if the request by User to enter a password, but also to continue to assess the camera frame. The system can identify the user when entering their credentials, This accelerates their access. As long as the user is still before the devices, systems and methods of the present invention attempts to perform Matching rows in the database. Even in the aftermath of authentication, use this feature to evaluate each successive authentication The camera frame.

After the image from the camera is converted to a vector image, the device then determines whether the vector A vector database identified match (211). If no match occurs and the user No reminder timer expires (221), the device continues to use the database to handle new vector Incoming image vector to determine if a match occurs. If the user reminder timer expires, then with After requesting the user's login credentials (at 223), where you can use the keyboard to enter the certificate, the user can Manually enter a password or other certificates, or other types of interfaces, such as other biometric party law. Meanwhile, the device continues to scan for new incoming image / vector to determine whether those in the database match. If a match occurs with the database at any time (in the 211), the system will continue to work with optional because Sub-match. If the certificate database and the user equipment is stored in the certificate does not match, then the process Start again, using this process, the device waits for initial login credentials from the user (203) and following Continued scan vectors.

However, if the certificate in the database matches the certificate, and certificate match with an optional factor factor Hotels (213), then start the process of automatic database as discussed in FIG. 3. Timing remind the user Before (221) expires, it received from the camera in the current vector and a vector database Case of a match, the user may be prompted one or more additional authentication factor, such as a pass phrase or Optionally provide additional factor for a second password authentication. If the user fails to provide this access If the pass phrase or phrase does not match the database phrase, the system returns to the beginning, User alerts timer is reset and started landing display screen (203).

Once the user is authenticated, the user is then authorized to access (at 215), and sign in to the whole device Ministry or restricted use of its features. As comparative prior art, the inventive aspects of the present invention is that once Users get access, you can continuously scan and authenticate users (217). Those skilled in the art will recognize To know, this continuous certification process enabling a user to leave the device, allowing the display screen is invalid, So the image on the monitor screen or can not be viewed, and the data item is locked. therefore, When the user leaves the camera's field of view can be easily protected equipment currently on display text, images, Or other data security. Once the user returns to the camera's field of view again, the method of the present invention provides The re-authenticated user. Once the re-certification, display and data items are locked, so that It allows the user to leave the field of view in a state such as when to access the device immediately.

In normal use, when using this method to protect the security of personal computers on the device Run application software is not affected, and continues to run on the device, although not shown. but, The method of the present invention allows the user to select the device when the device becomes locked or extent of the impact of unlocking. because Here, the user can use the device to make determination method 1) locked, 2) to unlock, 3) login, 4) Cancellation. Device "locked" provides secure desktop without causing user disconnects a document or e-mail Server, and do not close any application software running on the device. When the user is not depending on camera Baseball inside, the display device, a keyboard and / or mouse may be malfunctioning. Once the user back Vision method provides recertification. Once re-established this monitor safety, the equipment It can be used again. Thus, this procedure when the user is located outside the camera field of view, providing a dimension Retaining a simple manner a personal computer or other device security. Because the use of biometric facial and Continuously authenticate users, or when users temporarily leave your workstation for a long time, allowing users to rest assured Display data on the device and access to the network will be safe.

3 is a flowchart illustrating continuing certification program in Figure 2 briefly described. Continuing certification process is a key feature of the present invention, because it allows the user, after entering the camera field of view to be easily Recertification. When authorized and authenticated users access to unlock the device (303), continuing certification Process (300) begins (301). Using biometric facial feature tracking or recertification program To determine the user still exists in the camera field of view (at 305). In keeping system unlocked, allowing Recertification user to face the highest level of security. Conversely, by tracking

authenticated users Facial features, facial feature tracking allows the use of low CPU resources to achieve high security. In this article Discussed with reference to FIG. 5 facial feature tracking and continuing certification.

If authenticated user leaves the field of vision of the camera (307), an optional delay start lock Set the timer process (309). The lockout timer delay process 5 fully described with reference to FIG. in After the end of the process, the locking device (311). If the user enters the camera field of view (at 313), You need to determine whether the optional Quick Unlock timer has expired (at 315). If a rapid solution Lock timer, quick unlocking timer is usually transient, usually from 1 to 10 seconds. If the fast locking solution Timer has not expired, then use the existing face rather than any particular facial recognition to unlock the device (in 335). If the fast-lock timer has expired, the device recovery for continuous biometric authentication Scanning (317). Restart the user to change the timer (319), and determines from the camera The image is stored in the database and vector match (321). If the camera image is not Match any stored image, it is determined whether the user changes the timer has expired (323). in case Has not expired, the process in the image does not match the database continues to match the position of the image (321). If the user changes the timer has expired, continue scanning and biometric database to match and when Former user requests his or her certificate. If so, start automated database existed Cheng (329), which will be more fully described in Figure 4. If you enter his or her user certificate Before matching database and the user changes the timer has expired, perform automated database over Cheng (329). At the end of the process at the automated database, it will assume the user has been authenticated. system Or unlock the device (at 335), or alternatively the cancellation of locking the computer existing users (in 337). Then the system will automatically log on to the new user and the user's account without any additional recognition certificate.

If a start image does not match any of the database (321), you may optionally be prompted with Another factor user authentication, such as a password or passphrase other types. If the additional recognition Certificate factor did not match, continue uninterrupted biometric scans (317). If there is a match, The need to determine whether the existing authenticated user is just temporarily left the field of vision of the user. if you are an existing authenticated user, unlock the device (at 335). If it is not an existing user, set Preparation can be configured to unregister the existing user (337) and first start of the logon process (301), At this point the end of continuous certification process (339).

Figure 4 is a process used to fill the database and return can be used to improve the quality of a database Vector Press Timer (400) of the flow chart. Automated database is a process: by the In the process of using the system and the user to enter a password, or a few occur after the user changes the timer expires When the database is matched, will create or update the system database. Although initially requires a password, then automatically The purpose of the database is not allowed by the actual use of the specific data to fill in the registration process, In which users will eventually be able to stop using password authentication and by using facial biometric data, can The method of the present invention for authentication. Whenever it takes a long time to be used for data Library matching, by updating the database, the database can improve the quality and reduce the number for subsequent The amount of time the database match. This also applies to the face of the user over time various physical changes, including including aging, the lens changes color (tan), relative to the head position of the camera users, and change Of camera features, including lighting and a variety of environmental conditions. The purpose is to return to the Timer process Prior to the actual time of identification or authentication event with one or more images to update the database. This Allows user to access the device for the first time, the system can achieve higher weight closely match the user first site Opposing the image.

When receiving from the camera to the video frame (403), started automated database and return set Timer process (401). Start the user to change the timer (at 405) and needs to determine whether the image is A facial image. If it is not the facial image, the program returns to receive the video (at 403). Once seized We measured the face images, video frames and timestamp temporarily stored in a memory (409). Timestamp indicates the time from the actual camera image of a face. Compare this figure to determine the make Like a match in the database of another phase vector image. If a match, the user authentication (in 427). Without a match, the user needs to determine whether the change timer has expired (413). If the user changes the timer has not expired, and then view the images to determine whether the facial image (407). If the user changes the timer has expired, then the user is requesting user name and password, Password phrases (at 415). If you do not use the correct certificate for authentication (417), then See the image again to determine if it is a facial image (407). If the user is authenticated, the base The actual time minus the return authentication timer value to obtain an image (at 419) from the memory, because When a user requests to enter his or her credentials, is still receiving a video frame (403) and following

Continued database match (411), even if the user enters his or her certificate, the Department of The system can also make a match and proceeds down user authentication (407). The next step is to determine the user Whether pre-existing images in the database. If the user does not have previously stored in the database In the image, the user was to create a new database (at 423). Then, once the number of newly created Databases or pre-existing images are available, the image will get added to a user's database (in 425). Then authenticates the user (427) and ends the process (429).

5 is a diagram showing a continuous facial features for continuing certification embodiment of the present invention and tracking Delay lock process flow diagram (at 500). As facial features continuous tracking of authentication methods The advantage lies substantially to the central processing unit (CPU) and a load with respect to the camera user's face High tolerance of position. Because in a very short time be able to lock the system or boot system deregistration, Delay lock receiver allows the user to set how fast locking system to match the needs of the user. This A running process (at 215) immediately after the start of the accreditation until the locking device or log device. Such as if this condition exists, if there is to track the user's face or any mouse or keyboard activity, the system will Remains unlocked. This is desirable among as lock / logoff actions may occur too quickly. Not once Then detects mouse or keyboard activity before locking device, the method of the present invention provides an alternative The predetermined time period. If the user's face or to return to the field of vision if the inactivity timer expires Before restarting the keyboard / mouse activity, it will not lock the device and reset the timer.

More specifically, when the authorization authenticated users to access an unlocked device (503), start over Cheng (501). Receiving video frame (505) from the camera and placed into one or more tracking points The salient features of the user's face on (507). Then the number of tracking point counts (509) And the need to determine the current number of tracking points. If the tracking point meet the minimum threshold value, has been granted User access rights (503) and the lower device remains unlocked situation began the process again. If now The number of tracking point is below the minimum threshold, the start lock delay timer (513). Referring to Figure 6 more Fully describe the process of using a timer for locking delay. Next determine whether any of the mice , Keyboard activity, or other peripherals (such as activity on the touchscreen). If there is no activity, in the authenticated user is accessing the situation began again to unlock the device process (503). In case There is activity on the mouse or keyboard, it is determined whether the delay lock timer has expired (519). If the delay of the lockout timer has not expired, then re-start the process (503). If the delay Lockout timer has expired, the locking device (529) and ends the process (521).

Figure 6 shows a continuous biometric authentication & delay lock flowchart of FIG. 5 as in Continuous tracking of facial features shown and delay the process of locking an alternative embodiment 500. although Figure 6 is very similar to the method described in the tracking feature depicted in Figure 5, but continuous biometrics Certification provides better security in theory, because it constantly re-confirm the user. In fact, Continuous tracking of facial features would be so quick locking system so that new users difficult to lock in the system Before replacing the existing user. Continuous biometric recognition is very CPU-intensive, and It requires the user's face in front of the camera a more consistent replacement. These two factors make continuous Biometric understanding in many environments and devices less than ideal. Alternative implementation would include continuous Biometric authentication and continuous tracking of facial features a combination of both, which perform most of the time Facial feature tracking and biometric authentication in the run periodic intervals.

In Figure 6, the use of a continuous biometric authentication process and delay lock 600. When granted When users access rights to unlock the device (603), beginning of the process (601). Receive video from the camera Video frame (605) and determines whether the image matches the authenticated user. If the image does not match, In the case of users continue to access the unlocked device, the process starts again (at 603). If the image Authenticated user does not match the image, the start delay timer lock (609) and determines Whether there is any mouse or keyboard activity (at 611). If there is no activity and delay lock Set the timer has expired (at 613), equipment or cancellation device (615) and the program will be locked End (at 617). If there is no activity (611) and lock delay timer has not expired (in 613), the device is started again (603). If there are active (at 611) the timing or delay locking Does not expire (at 613), then the process starts again (at 603).

Figure 7 shows an extension is based on an alternative embodiment of the present invention is a system and method of the present invention. Flutter block diagram, in which screen mode and / or gesture mode and the camera is used to provide users with system recognition certificate. First, those skilled in the art would recognize that those types of "tolerance" factor can tolerate input or factor, because they can be accepted without having to provide secure access to an electronic device

registration Ensure accuracy. In other words, an exact match may not be necessary, just the opposite is some predefined Matching similar manner. Therefore, can be selected and / or adjusted so that a particular factor "accurate" Factor means that their matching tolerance must be accurate and / or substantially precise to allow access equipment. Tolerance or accuracy factor rating will normally run correctly chosen by the manufacturer of the software; However, the combination of these types of factors allow to provide great security apparatus and method simultaneously Ease of use and user access.

1 according to system 700 includes each of the components described in FIG; however, the connection device further comprises To the electronic device 701 or touchscreen 701 used in the electronic device 709. Although it is shown using isolated Keyboard 703, those skilled in the art will recognize that the keyboard 703 may be formed using software virtual Touch screen 709 is integrated into the keyboard, so that the keyboard 703 and 709 can be used as a touch-screen device. Such as This paper points out, the touch screen 709 in conjunction with the camera 711 to operate, the camera 711 is input by the microprocessor Processor 705 control and interpretation. This allows users to enter in touch gesture 709, the gesture imaging Head 711 in combination to provide user authentication for the device. These inputs are stored in the database 713 Data and other information in comparison. This data is used by the comparator 715 to compare the ratio Compared with 715 for providing access to comparative analysis of the type of operation to access the electronic device 701. As described herein Described later, the tracking feature 717 can also optionally be used to ensure that the user equipment is maintained in the same individual, and in No security gaps and vulnerabilities.

8 is a diagram showing a screen for providing a user mode / gesture and facial biometric both Flowchart of an embodiment of another electronic device alternative. Use screen gestures and facial biometrics Both certification process (800) comprising the steps of starting the initial "Sign in" process (801), and The step 801 is triggered by some external event requiring the user to enter the certificate. Then display certification Screen (in 803) and the camera receives at least one video frame (805), so that the user can Then enter predefined screen gestures or other safety factor (at 807). Although in practice, Users of one or more factors such as security before other factors happen, but the art Any technology will further recognize that in the process of the present invention, these factors do not need to occur simultaneously or Occur in a specific order. In fact, since the start-up delay of the camera, this step can be first If happens, but this is not necessary.

Then, you need to determine whether the received frame by the camera and facial recognition cloud or local data matches Hotels (809). Those skilled in the art will recognize that "cloud computing" means via a digital network Using multiple server computers, it may seem like a computer. Can via the Internet Etc. using a computer to access the cloud. If the number of attempts or other data over a number of Predetermined period of time or some of the counters (at 811), it requires the user to enter alternative credentials or cancel Request (at 815). If no more than the counter, the camera will be used to provide additional video frame (At 805). Once you enter the alternative certificate, you need to determine whether the data is stored certificate Library that matches the certificate (817). If the certificate matches, automated database is performed Procedure to update the stored images and / or other data (819) in the database. If the certificate does not match Hotels, then the camera is used to provide additional authentication of video frames (805).

When the gesture with clouds or local database does not match (at 813), then again it may require user input Replace or cancel a certificate request (at 815). If the new certificate does not match in there from a camera At least one of the first new frame (805), the process starts again; however, if the new certificate is not Match, then perform the update of the automated database updates facial biometrics (819). but, if the gesture match (at 813), the authentication of the user and their local or cloud-based certificates in To a specific application for authorization to access and / or use (in the 821). Any update biometric facial Data will be used in a certification process (in 821) in. Therefore, how to clear the screen (at 823) And the process ends (825).

In typical use, a user needs to access the device smart phone or any device on the certification Or applications that require authentication. The certification is usually required to enter a user name and password. By using embedded Positive type image forming apparatus (for example, a camera) get facial recognition template for software certification. Big At about the same, the user is prompted to enter their previously registered gestures. The face and gesture registered user to Template database before registration for comparison. At the same time biometric facial data by almost And compare gesture, reducing the matching tolerance of each factor, without reducing safety reliability. Because greatly reduced will usually result in a face recognition or gesture recognition and often less credible Situation is causing real user undesirably wrongly rejected, so this greatly improves the user experience.

Those skilled in the art may recognize that many different variations further gestures and biometric information Type (e.g., accuracy / tolerance factor and a plurality of tolerance factors) may include, but are not limited to:

Accurately factor and tolerance factor

Password and face

Password and gestures

Password and Pattern

Password and fingerprint

Personal identification number and face

Personal identification numbers and sounds

A plurality of tolerance factor

Face and Gesture

Face and part of the password (for accepting to reduce the number of password characters)

Face and patterns

Face and fingerprint

Face and voice

Face, voice and gestures

And shape of the face

Shapes and gestures

Login name and password, according to various embodiments of the present invention, instead of using assigned, as described herein Using the method described in the user's face unique, individual features combined with personal identification numbers, gestures (with User activity patterns selected for its finger on the touch screen) or display symbols, or other shapes A combination of markers to verify identity and to provide safe and convenient access. This not only provides a new method Easy access and easy to solve the embodiment described herein, input fast and stress-free The way to ensure that two-factor authentication problems.

Accordingly, the present invention can also provide personalized, cloud-based password safe, convenient and Universal "Single Sign On" (single login multiple applications and devices). As described herein, the user Type are known and have many letters, numbers, shapes or other indicia of a password to gain access. From Any device password stored in the safe at any place and on any other device can immediately Too, and you can be cached on the local device. The advantages of cloud-based storage is that all information Before it is used it is always encrypted. Embodiments of the present invention further comprises means for Windows, iOS, And other multi-platform Android operating system device support. In addition, the password can also be stored in the cloud And the center is fully encrypted. Another advantage of this arrangement is that the device (phones, computers, flat Board computers, etc.) can be damaged, lost or reload, but will remain on the database user authentication Accessible. Next, the present invention allows multiple users to safely separated from one another and share a single Mobile devices. Each user has its own private memory storage areas or password only through personal CD A face and gestures available "safe."

Because PC with reduced mobility and are typically used only at a limited number of positions, so this Types of permit conditions set for more intolerance identify matching requirements. In this setting, PC typically has a very low rate of error reported in the error message 106 access attempts on / in of only about 6.3. Thus, in the PC environment, after a brief period of study, at the same time get a good recognition rate To maintain high accuracy. However, the typical PC environment illumination and observation of the face with respect and Relative to control. This does not apply to the case of mobile devices, including mobile devices due to the lighting and The camera angle of the face / face distance from the camera has a high respect differences, lighting and so Handheld mobile devices is always observed on the face of significant changes. In order to

maintain this changing environment Very high recognition rate, matching tolerance must relax a little in order to provide good recognition rate. Unfortunately it is relaxed tolerance also increases the possibility of incorrect identification. Even casual users will not be tolerated High error rates, and will lead to the identification unauthenticated access to their private data.

The use of secondary factors, such as face recognition mode is when, exponentially increasing the quasi certification Accuracy, thereby simultaneously input mode / personal identification number, and the face recognition is very fast, natural and convenient. This allows the embodiment of the present invention, the face recognition matching tolerance value, which provides changing lighting situation Excellent condition and identify the various angles of the face, while improving the overall accuracy of authentication than most Points authentication scheme. Use face recognition and gesture, you can minimize both the disadvantaged. In the face recognition Under other circumstances, a gesture to prevent attacks photo or video, and face to prevent another user authentication simply Observation and repeated gestures. Therefore, the success of "smear attack" in the absence of face case essence You can not be accessed. Successful "replay attack" (photo / video) can not be performed without the use of gestures access. Having a plurality of factors also helps to minimize social engineering. When having all forms of security / secret When the density of the user's personal understanding will increase access to unauthenticated access speed. It requires multiple independent Li type of information reduces any individual article will be enough individuals to understand this possibility.

9A and 9B shows a display arrangement features dynamic gesture touchscreen. 9A shows when Paintings region is maintained at the same or identical positions on the touch screen surface or residue left finger painting Appearance. Because of the residual pattern, and the residue may allow unauthenticated observed that given by Households gesture, reduce the security of the factors. 9B shows a layout using dynamic gesture, that is, when If necessary gestures, the method of the present invention, a mobile gestures on the touch screen display to enter each point carefully Arrangement. Data on the display can be moved into the area and / or along any dynamic display Skew direction, such as up, down, sideways, or diagonally. This process allows overlapping traces of oil, This greatly reduces the possibility of being able to infer gesture certified personnel. This eliminates the common mode security Weakness, that means the oil from the oil traces on the device's screen, or other residue can be used as a display or implied in gestures or finger movement mode.

Figure 10 shows a combination of a plurality of permanent computer according to the present invention EXAMPLES readable medium A flowchart of the certification process. 1000 certification process begins: with live video and touch screen Display data input or "gesture" message prompts the user area (in 1001). OK imaging Head resettlement timer has expired (in 1003). If not, the process continues until the camera is Capturing one or more images while still fully booked up period. Once the timer has expired, that What the user's image is captured and transferred to the user on the touch screen electronic devices (in 1005). another in addition, the user can display the "Start Scan" Animation for providing video capture authentication notice But also can display a variety of other indicators on the screen. To capture a predetermined number of pixels or the frame, increase the retry counter, and sends the image to a predetermined position for evaluation.

Then, determine whether the user is invalid, also known as "bad user" (in 1007). If Household invalid or bad (in 1009), then the display will notify the user requires an initial "build" System or software program (in 1009). In this case, the user steps leading to the establishment of secondary (In 1011). However, if the user is not valid, then the process determines whether the user is detected Face (in 1013). if detected, the face image is saved for later learning step (in 1015), and by comparing the face data stored locally or in the cloud database to determine the face Whether certified (in 1017). If the face is certified, the process continues to determine whether the input The second factor (in 1039). As described herein, the "second factor" is a gesture or article Enter on the touch display of the symbol combination described herein. However, if the face unapproved Card (in 1017), the system determines whether it has exceeded a retry count (in 1019). If it does not exceed Retry count, the system informs the user that it is not recognized (in 1037) and by prompting the user again Beginning of the process (in 1001).

If it exceeds the retry count (in 1019), the system determines whether to save the image for later Learning step (in 1035). If you save an image, the user input is used to remind the user to learn the face Cloud password portion. Thereafter, the processing and storage of the user face image (in 1036). This process will be retried (In 1038) and enter the cleared state (in 1044), or if you enter a valid password (in 1040), Images are saved in a systematic process for "learning" step (in 1042). Determining the effective user authentication (In 1029), to authorize user access to the electronic device (in 1031). If you do not save the image (in 1035), this will trigger a network or a network timeout error message (in 1023), and the user canceled Face authentication

processing step. Thereafter, the user is prompted for a password override (in 1025). Once you have entered and Recognized as a valid password (in 1027), you can launch an effective authentication command (in 1029), and authorized Users access the electronic device (in 1031).

It should be noted at this, the event of the face authentication (in 1017), then a second confirmation Whether the user has entered the second factor (in 1039). The second factor may include, but are not limited to screen Gestures, passwords, display input and various combinations of symbols. If the second factor is invalid (in 1041), the user is prompted to re-enter the personal identification number of gestures (in 1043), and the process Start again (in 1039). However, once the second factor is effective (in 1041), then the user Show approval or confirmation (in 1045), and the user certificate is valid, thus authorizing them to visit Q. electronic equipment (in 1031).

Therefore, as in the process of overwriting the password, the method of the present invention (1025) provided as described "Back" access operation, can not happen in the case of the "standard" certification (for example, if Due to the extreme lighting conditions can not be face recognition), single or multi-factor can be overwritten of. You can set the override and complex requirements for each factor to meet the desired security objectives. Override options include, but are not limited to, the following entries: Personal identification Number (PIN); screen gestures and PIN; Complex password (letters, data, and / or symbols); or screen gestures and complex passwords.

Sometimes store sensitive information is a cause for concern in the cloud, it is usually necessary to carefully consider. This is because the authentication information is not destroyed for the purposes of operating system is disadvantageous. According to another of the present invention A program can take advantage of Rijndael with a fixed block size, and repeat count of at least 128-bit key Symmetric algorithms, on the cloud server and / or local electronic devices certificate for encryption. The encryption technology Usually more than the standard for government and financial data. Use unique encryption key for each user, The Web site certificate to encrypt "data in a binary large object (data blob)". Thus, in a user's Under impossible circumstances account been compromised due to other than the user of the other party does not know the encryption Key or password, so the key can not be used to access other users' data. Since the key information can be Remains unknown, it is always recommended to back up the certificate in the local database. Due to recover passwords from the cloud is Impossible, so never unencrypted state transfer data. In fact, not until before use Presence unencrypted. In this configuration, the electronic device (phones, tablets, laptops, etc.) Simple or "dumb" client usually does not store data locally on it. This means Even if the device is stolen, no matter how much effort spent hackers, passwords can not be physically presented. Have Time limit local cache is optionally available, which allows the administrator to the present invention can, if necessary, From the network operation, while minimizing risk.

Therefore, the system and method of the present invention to provide a personal computer or other safety requirements Fast, simple and secure access to electronic equipment. The present invention incorporates the use of hands in the authentication process screen Potential and biometric security. By combining the almost simultaneous analysis of at least two factors, can be reduced Tolerance factor required tolerance matching, without reducing the overall accuracy of electronic security equipment. Health binding Biometric technology at this level of security means, the present invention provides a unique use of multiple platforms Security certificates to obtain cloud-based rapid and accurate log into the device, websites and app, and personalized Access devices, such as Android and iOS without user account. With the embodiment of the present invention uses Imaging illumination tolerance for unwanted images provide very strong photos and videos rejected.

While there have been shown and described a preferred embodiment of the present invention, it is clear that the present invention and Is not limited thereto. In the spirit and scope of the appended claims without departing from the present invention, The skilled artisan can envision a variety of modifications, changes, variations, subsitutions and equivalents. Such as As used herein, the term "comprising", "including" or any other variation thereof are intended to cover a non- Exclusive inclusion, so that process, method, article, or apparatus comprising a column member that includes not only the These elements, or may also include such process, method, article, or apparatus not expressly listed inherent The other elements.

Patent Translate
Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

CLAIMS CN103593594

1.

1. A method for providing security for electronic equipment biometric facial recognition system, comprising:

Digital cameras, a user from having to provide the electronic device for establishing a first View of a plurality of biometric facial image of safety factors;

A touch screen for enabling the user to input the safety factor for establishing a second data;

With the at least one processor associated with the electronic device, for connecting the first and the factor Said second factor data stored in the database for comparison; and

Wherein, if the data of the first factor and the second factor stored in the database Match, enabling access to the electronic device.

2.

2. Facial biometric identification system as claimed in claim 1, wherein, said touch-screen Data input area can be dynamically configured to prevent the input before the residue is identified by a finger The data.

3.

3. Facial biometric identification system as claimed in claim 1, wherein said second factor is a screen gestures.

4.

4. Facial biometric identification system as claimed in claim 1, wherein said second factor is a predetermined combination of symbols displayed.

5.

5. Facial biometric identification system as claimed in claim 1, wherein said position database Within the electronic device.

6.

6. Facial biometric identification system as claimed in claim 1, wherein said database is cloud.

7.

7. Facial biometric identification system as claimed in claim 1, wherein said electronic device It is set from the personal computer, personal digital assistant, a mobile phone or a gaming device.

8.

8. To provide a secure method for an electronic device, comprising the steps of:

Authentication screen display;

Providing data from at least one camera for providing a biometric authentication data;

Provide user input data to the touch screen display;

The biometric authentication data and information stored in the database for comparison;

The user input data and information stored in the database for comparison;

Determining whether the user is authenticated;

If the user is authenticated, then to run the application on the electronic device to input authentication certificate Books; and

Unauthorized access to the electronic device.

9.

9. The method for providing security according to claim 8, further comprising: said user The step of the face is used as biometric authentication data.

10.

10. The method for providing security according to claim 8, further comprising: a screen gestures The step of the user is used as input data.

11.

11. The method for providing security according to claim 8, further comprising: using the A predetermined sequence of steps on the touch screen display of the symbol.

12.

12. The method for providing security according to claim 8, further comprising: the touch The shape of the steps as a plurality of symbols displayed on the screen display.

13.

13. Moving the contact: the method for providing security according to claim 8, further comprising Data entry fields on the touch screen display shows, in order to prevent the stay on the touch screen display Before the next step and the residual recognizes the input data.

14.

14. The method for providing security according to claim 8, further comprising: selecting Said biometric authentication data or the user input to provide any of a tolerance factor to use For if the comparison is within a predetermined tolerance is authorized to access the electronic device steps.

15.

15. The data: a method for providing security according to claim 8, further comprising Library includes the step of the electronic device.

16.

16. The data: a method for providing security according to claim 8, further comprising Internet access is included in the library via cloud steps.

17. The method as claimed in claim 8, wherein said electronic device is from a personal computer Machine (PC), a personal digital assistant (PDA), cellular phones, gaming devices or mobile phone group one of.

(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103593594 A
(43)申请公布日 2014.02.19

(21)申请号 201310008147.0

(22)申请日 2013.01.09

(30)优先权数据
61/584,492 2012.01.09 US

(71)申请人 明智视觉有限公司
地址 美国密歇根州

(72)发明人 C·阿扎尔 G·布罗斯托夫

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 王英 刘炳胜

(51)Int.Cl.
G06F 21/32(2013.01)
G06F 21/31(2013.01)

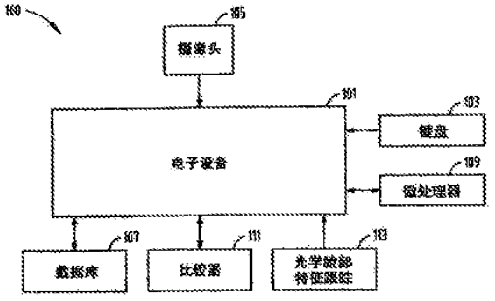
权利要求书2页 说明书12页 附图10页

(54)发明名称

用于使用脸部生物特征识别和屏幕手势来提供对电子设备的安全访问的系统和方法

(57)摘要

一种用于向设备提供安全认证的系统和方法(800),其包括:将两个或更多个安全因子组合以用于大约同时操作的认证的步骤(805、807),其中至少一个因子是"容忍"因子。通过将大约同时分析的两个因子进行组合(805、807),可以减小容忍因子所需要的容忍匹配,而不降低总安全精度。



CN 103593594 A

1. 一种用于为电子设备提供安全的脸部生物特征识别系统，包括：

数字摄像头，具有用于提供来自所述电子设备的用户的用于建立第一安全因子的多个脸部生物特征图像的视野；

触摸屏，用于使得所述用户能够输入用于建立第二安全因子的数据；

与所述电子设备相关联的至少一个处理器，用于将所述第一因子和所述第二因子与数据库中存储的数据进行比较；并且

其中，如果所述第一因子和所述第二因子与所述数据库中存储的数据相匹配，则使得能够对所述电子设备访问。

2. 如权利要求 1 所述的脸部生物特征识别系统，其中，所述触摸屏上的数据输入区域能够被动态地设置，以防止通过手指残余面识别之前输入的数据。

3. 如权利要求 1 所述的脸部生物特征识别系统，其中，所述第二因子是屏幕手势。

4. 如权利要求 1 所述的脸部生物特征识别系统，其中，所述第二因子是所显示的符号的预定组合。

5. 如权利要求 1 所述的脸部生物特征识别系统，其中，所述数据库位于所述电子设备内。

6. 如权利要求 1 所述的脸部生物特征识别系统，其中，所述数据库是云。

7. 如权利要求 1 所述的脸部生物特征识别系统，其中，所述电子设备是来自个人计算机、个人数字助理、移动电话或游戏设备的组中的一个。

8. 一种用于向电子设备提供安全的方法，包括以下步骤：

显示认证屏幕；

提供来自至少一个摄像头的数据，以用于提供生物特征认证数据；

向触摸屏显示器提供用户输入数据；

将所述生物特征认证数据与数据库中存储的信息进行比较；

将所述用户输入数据与数据库中存储的信息进行比较；

确定所述用户是否被认证了；

如果所述用户被认证了，则向所述电子设备上运行的应用输入认证证书；以及

授权对所述电子设备的访问。

9. 如权利要求 8 所述的用于提供安全的方法，还包括：将所述用户的脸部用作所述生物特征认证数据的步骤。

10. 如权利要求 8 所述的用于提供安全的方法，还包括：将屏幕手势用作所述用户输入数据的步骤。

11. 如权利要求 8 所述的用于提供安全的方法，还包括：使用在所述触摸屏显示器上显示的符号的预定序列的步骤。

12. 如权利要求 8 所述的用于提供安全的方法，还包括：在所述触摸屏显示器上显示作为所述符号的多个形状的步骤。

13. 如权利要求 8 所述的用于提供安全的方法，还包括：移动所述触摸屏显示器上所显示的数据输入区域，以防止由于所述触摸屏显示器上留下的残余面识别之前输入的数据的步骤。

14. 如权利要求 8 所述的用于提供安全的方法，还包括：通过选择所述生物特征认证数

据或所述用户输入中的任何一个来提供容忍因子，以用于如果所述比较位于预定容忍内则授权对所述电子设备的访问的步骤。

15. 如权利要求 8 所述的用于提供安全的方法，还包括：将所述数据库包括在所述电子设备中的步骤。

16. 如权利要求 8 所述的用于提供安全的方法，还包括：将所述数据库包括在经由互联网访问的云中的步骤。

17. 如权利要求 8 所述的方法，其中，所述电子设备是来自个人计算机（PC）、个人数字助理（PDA）、蜂窝电话、游戏设备或移动电话的组中的一个。

用于使用脸部生物特征识别和屏幕手势来提供对电子设备的安全访问的系统和方法

[0001] 本专利申请要求于 2012 年 1 月 9 日提交的临时专利申请序列 No. 61/584,492 的权益和优先权，该临时专利申请的公开内容通过引用方式并入本文。

技术领域

[0002] 本发明一般涉及电子安全，并且更具体地涉及使用屏幕手势和脸部生物特征来认证电子设备的用户的方法。

背景技术

[0003] 许多电子设备（例如个人计算机、包括移动电话和个人数字助理（PDA）的移动设备）使用某种形式的认证（通常是必须输入到设备中的密码）来获得访问。最经常的是，密码被键入到键盘或其它接口上，其随后允许用户获得对设备和 / 或网络的功用的部分或全部访问。与使用密码相关联的问题在于它们是耗时的，并且对于用户进行输入来说是不方便的。用户常常使用非正式的密码或与他人共享他们的密码，这危害了系统的安全。这些实际情况否定了密码的价值，并且使得难以精确地对访问进行审计。此外，密码在被忘记、与他人共享或放错位置时管理起来是昂贵的。虽然已经实现了使用其它类型的安全访问系统，例如语音识别、指纹识别或虹膜扫描，但是这些类型的系统需要不同的过程来访问以及使用设备。为了能够操作，这些技术还需要特定的并且耗时的登记过程。

[0004] 因此，“身份管理”总是呈现出挑战。开始，个人已经与用户名和密码相关联以便获得对计算机系统的访问，这产生了对认证（验证个人是“他们所声称的真正的人”）的显著挑战。这通常意味着要记住并输入用于计算机、安全应用以及多个网站的唯一用户名和密码。对于需要额外的安全控制的系统（例如，在线银行）而言，已经要求个人使用“两因子认证”。这需要多个类型的标识，例如密码加 PIN 或令牌。随着用户不断地使用多个电子设备和服务（例如，智能电话、电子邮件、在线银行、社交网络），记录多个密码并不断地输入这些密码已经简单地变得在最好的情况下是不方便的，并且对于许多情况而言是不可管理的。几乎每天，新闻都与我们分享着网络犯罪如何提高了这种挑战，……，从而强制使用更长的、更复杂的密码，这些更长的、更复杂的密码必须被频繁地更改或者冒着丢失重要信息、隐私、名誉和金钱的风险。增加的复杂性并不鼓励强安全措施和策略的使用以及与这些措施和策略的符合。受挫的用户本身可能就面临着安全风险。

[0005] 使用脸部识别的生物特征认证经常用于获得对电子设备的访问。授权给 Kyle 的美国专利 No. 6,853,739 和授权给 Akiyama 等的美国专利 No. 6,724,919（这两个专利通过引用方式并入本文）公开了身份验证系统的例子，在这些身份验证系统中，采用数据库来将用户的脸部特征与预先建立的数据库中的那些特征进行比较。一旦进行了比较，随后就对认证进行验证，并且授权对系统的访问。这种类型的系统的缺点在于需要用户进行单独的并且特定的登记过程以便建立数据库。就这种类型的脸部识别系统以及现有技术中的其它系统而言，数据库必须在使用之前被填充；否则，系统将不会操作。这给系统操作员施加了

不必要的负担，需要关于在系统可以变得可运行之前填充数据库的步骤的详细培训。另外，这种类型的安全系统并不允许自动地更新数据库以适应头部位置、用户特征(例如不同的眼镜)的改变、摄像头操作特性、灯光以及其它环境因子的改变。这可能限制了数据库匹配(识别)的速度、精度以及甚至成功性。而且，这些现有的脸部识别和其它生物特征系统仅仅在认证时刻进行运行。

[0006] 其它技术使用与设备的显示器相关联的手势。这种类型的识别技术涉及用户触摸设备的触摸屏以及被设备识别的移动。这些移动可以链接到设备功能，例如某些应用的运行或允许对设备的访问。手势是用户的手指在触摸屏上的移动，所述移动的模式或形状是用户已经标识或选择的。某些因子依赖于精确的匹配，而其它因子由于其设计的特性而使用某种级别的匹配容忍(也称为容忍因子)来确定手势或证书的接受。精确因子的例子包括用户的完全密码、智能卡或来自硬件安全令牌的代码。这些因子必须总是精确地域之前存储的证书相匹配。容忍因子包括所有形式的生物特征(脸部、语音和手指)、与同所存储的证书的精确匹配存在某种定义的偏差 / 容忍被允许(并且实际工作也是需要的)的模式和手势。甚至是如果在某些情况下接受比总长度小的密码，那么密码也可以变成容忍因子。

[0007] 使用生物特征来补充密码输入的安全系统的另一例子是授权给 Hwang 等的美国专利 No. 7, 161, 468。该专利中描述的是一种用户认证设备，其基于用户输入的密码以及用户的生物特征信息来认证用户。该用户认证设备包括：密码输入单元，其确定是否已经输入了密码；存储单元，其存储已注册的密码和已注册的生物特征；阈值设定单元，如果输入的密码与已注册的密码匹配，则所述阈值设定单元设定第一阈值，并且如果输入的密码与已注册的密码不匹配，则所述阈值设定单元设定第二阈值；以及生物特征单元，其从外部获得生物特征信息，确定所获得的生物特征信息与已注册的生物特征信息的匹配程度，并且如果所获得的生物特征信息与已注册的生物特征信息的匹配程度大于第一或第二阈值，则认证用户是真的。作为在本发明的范围内如何调整这种系统的例子，生物特征输入可以用隐藏的动作进行补充，以便遵守之前配置的规则而完全地认证用户或传递辅助密码和相关联的动作，例如账户约束、虚构访问或警告发布。

[0008] 最后，Lin 的美国专利公开 No. 2009/0160609 描述了一种对锁定的计算设备进行解锁的方法，其中，用户的触摸用作对设备进行解锁的请求，而生物特征信息可以与该过程一起使用。虽然用户可以使用触摸屏来请求对设备进行解锁，但是 Lin 并没有使用屏幕手势和生物特征信息的组合来认证用户。

[0009] 因此，虽然在本领域中，手势和生物特征安全系统的使用是单独可用的，但是当前并不存在将这些技术组合起来以提供鲁棒的安全性同时还向用户提供灵活的对电子设备的访问的系统。

附图说明

[0010] 图 1 是示出了本发明的系统和方法的拓扑的方框图，其中，使用摄像头来向用户提供系统认证。

[0011] 图 2 是示出了使用脸部生物特征的方法的概述的流程图。

[0012] 图 3 是示出了根据本发明实施例而使用的连续认证例程的流程图。

[0013] 图 4 是示出了根据本发明实施例与自动数据库一起使用的后定时(back-timing)

过程的流程图。

[0014] 图 5 是示出了根据本发明实施例而是用的脸部特征跟踪和延迟锁定子例程的流程图。

[0015] 图 6 是根据本发明而是用的、图 5 中所示的生物特征认证和延迟锁定例程的替换实施例的流程图。

[0016] 图 7 是示出了根据本发明替换实施例的本发明的系统和方法的拓扑的方框图，其中，使用屏幕手势和摄像头来向用户提供系统认证。

[0017] 图 8 是示出了利用屏幕手势和脸部生物特征提供对电子设备的认证的另一替代实施例的流程图。

[0018] 图 9A 和 9B 示出了展示动态手势放置的特征的触摸屏。

[0019] 图 10 是示出了使用脸部识别和其它因子以认证用户访问电子设备的流程图。

具体实施方式

[0020] 本发明关闭对于需要安全访问的所有类型电子设备来说以多种现有安全认证形式中存在的基本安全漏洞。现有的安全方法仅确认用户输入其密码、扫描器指纹或虹膜时刻的用户。系统不能分辨当前用户是否是几毫秒之前认证的同一个体。这使得设备非常不安全并且是脆弱的，直到注销设备或者锁定。对于怀有恶意的人来说，仅需要花费很少时间就可以盗取和 / 或删除用户已经登录的设备的数据。现有的方案要求用户手动锁定 / 注销，或者生成用户不活动计时器来锁定或注销用户。

[0021] 此外，大多数信息技术（IT）组织不愿意改变，因为他们不愿意冒风险改变，这会影响其现有的硬件 / 软件系统。此外，他们不愿意增加实施这一方案所需的支持成本。用于训练用户和回答帮助桌面问题的支持成本会是很大的因子。本发明可以用对终端用户透明的方式自动生成数据库。本发明需要很少的训练并且成本很少的“桌面帮助”。本发明使用自动登记特征，其允许设备自动更新数据库来不断改善用户识别质量。相反，当前生物特征产品需要一组特定步骤来建立并更新数据库。在一些情况下，仅在初步学习之后，可以由用户执行这些步骤。在许多情况下，在系统中使用之前，IT 管理者必须与用户一起工作来实际训练数据库。

[0022] 符合安全也是一个重要问题，当其远离计算机时，通常需要用户手动锁定或注销其计算机。这一过程很花费时间、并且不方面，对于使用计算机过程中用户目的来说是次要的。此外，锁定或者注销使得当用户返回设备时输入密码，这带来很大不方面。除非严格实施，用户通常忽略这种正确的安全过程。在缺少直接监管下，对于系统管理员来说，本质上没有办法确认用户是否正确地遵守指定安全策略。

[0023] 一个不切实际的方案通常包括使用计时器。当在预定时间段内没有外设活动时通过锁定设备来使得计时器工作。如本领域技术人员所认识的，外设可以包括，但不限于鼠标、键盘或触摸屏。如果计时器被设置为足够短的持续时间来在用户离开设备时适当关闭安全漏洞，那么设备将在用户查看屏幕上的数据时锁定。每次洗头锁定或者注销用户时，用户需要不断输入其证书。这导致用户产生挫败感，并且大大降低生产率。因此，通常不活动时间至少为 2-5 分钟，这提供了很大的易受攻击的窗口。此外，不活动计时器是无效的。所有未授权用户必须在计时器时段内访问系统。在此之后，未授权用户可以无限期继续工作。

[0024] 本发明的系统和方法通过自动处理直接解决这种合规问题，因此确保完全合规。因为处理是自动的并且对操作者是透明的，用户接受度非常高。用户发现在安装本发明之后系统更便于使用。此外，示出了访问设备的人的系统核查日志现在是准确的，因为这种连续认证安全处理。本发明通过当用户在设备的视野之外时立即锁定 / 注销，然后在用户重新出现在计算机之前时尽快解锁来进行操作。

[0025] 现在参照图 1，如根据本发明使用的系统 100 包括电子设备 101，其包括但不限于个人计算机、移动电话、按字母排序分页设备、个人数字助理（PDA）、电子游戏设备等，这都需要某种类型的认证来获得对设备 101 的使用的访问。摄像头 105 还可以用于向设备增加额外的安全级别，其中所述设备的摄像头与设备 101 一起使用以利用多个图像矢量构建内部数据库 107。摄像头基本上提供实时图像并且通常以大约每秒 5-10 帧的速率运行，从而向电子设备 101 连续供应数字图像数据。摄像头通常与通常在设备内使用的光学脸部特征跟踪软件一起使用，其中所述设备用于当位于摄像头前面的位置时跟踪用户脸部的运动。因此，当用户使用设备时，将他的头前后左右移动，与摄像头一起使用的软件将跟踪脸部运动以允许连续认证，同时使用较低 CPU 和设备资源 113。

[0026] 本领域技术人员将认识到，摄像头 105 可以被整合到电子设备 101，或者其可以独立作为附件或外设，用于通过有线或无线连接将图像数据发送到电子设备。如本发明优选方法所描述，微处理器 109 与比较器 111 一起使用，从而确定摄像头 105 连续供应的图像是否是人脸图像。如果检测到人脸图像，则可以确定该图像是否与先前用户期间数据库 107 中存储的那些图像中的任一图像匹配。每个矢量表示从摄像头 105 发送到电子设备 101 的数字图像的数值表示。如本文所讨论的，电子设备 101 对数据库 107 中建立的矢量和摄像头 105 提供的当前矢量进行比较。当肯定地确定其匹配并且用户被认证时，系统 100 配置为允许用户可以对电子设备 101 完全或受限地访问。

[0027] 图 2 是示出了根据本发明的实施例的脸部生物特征方法 100 的总体的流程图。尽管本方法如图 2 中的序列所描述，但是对于本领域技术人员来说，在不脱离本方法的精神和范围的情况下，其它重用和定义是可行的，这是显而易见的。这些方法可以包括，二维（2D）、三维（3D）红外线（IR）和 / 或其它脸部识别技术，但并不限于此。在用于脸部生物特征概述 200 的方法中，在 201 开始用于登录设备的初始启动过程，设备显示器幕 203，从而允许用户提供其登录密码或其它认证证书。在 205，从与设备相关联的摄像头接收视频帧，其中在 207，通过使用脸部检测，利用该设备确定从摄像头接收的图像数据是否是脸部图像。如果不是脸部图像，那么设备继续等待用户登录证书（在 203）。

[0028] 不过，如果图像数据是脸部图像，那么用户提醒计时器启动（在 209）。用户提醒计时器用于确定某一预定时间，其中在该时间内，用户应当在向用户显示消息以请求用户手动输入其证书之前被认证。用户提醒计时器的期满，不同于推荐用户手动登陆，不对认证有影响，因为认证过程已经超过预期持续时间，并且系统将受益于数据库更新。因此，即使如果请求用户输入密码，也能继续评估摄像头帧。系统能够在输入其证书时识别用户，这加速其的访问。只要用户仍然在设备之前，本发明的系统和方法尝试执行数据库匹配。即使在发生认证之后，利用这一连续认证特征来评估每个摄像头帧。

[0029] 在来自摄像头的图像被转换到图像矢量之后，设备随后确定矢量是否与数据库中已确定的一个矢量匹配（在 211）。如果没有发生匹配并且用户提醒计时器没有到期（在

221），那么设备利用数据库中的矢量继续处理新进入的图像矢量以确定是否发生匹配。如果用户提醒计时器到期，那么随后请求用户的登录证书（在 223），其中可以利用键盘输入该证书，用户可以于动输入密码或其它证书，或者其它类型的接口，诸如其它生物特征方法。同时，设备继续扫描新进入的图像 / 矢量以确定是否与数据库中的那些匹配。如果在任意时间与数据库发生匹配（在 211），系统将继续与任选因子的匹配。如果用户设备的证书与数据库中存储的证书不匹配，那么过程再次启动，利用该过程，设备等待来自用户初始登录证书（在 203）并且继续扫描矢量。

[0030] 不过，如果证书与数据库中的证书匹配，并且与任选因子证书因子匹配（在 213），那么开始如图 3 所讨论的自动数据库过程。在用户提醒计时器到期之前（在 221），在从摄像头接收的当前矢量与数据库中的一个矢量匹配的情况下，可以提示用户一个或多个额外认证因子，诸如通行短语或者提供任选额外的因子以供认证的第二密码。如果用户未能提供这一通行短语或者如果该通行短语与数据库中的短语不匹配，那么系统返回到开始，用户提醒计时器被重置，并且显示开始登陆屏幕（在 203）。

[0031] 一旦用户被认证，用户随后被授权访问（在 215），并且登入设备来全部或受限地使用其特征。如对比现有技术，本发明的创造性方面为，一旦用户获得访问，可以连续扫描并认证用户（在 217）。本领域技术人员将认识到，这种连续认证过程使得用户能够离开设备，从而允许显示器幕无效，于是屏幕或监视器上的图像不在能够被查看，并且数据项被锁定。因此，在用户离开摄像头的视野时，可以容易地保护设备上目前显示文本、图像或其它数据的安全。一旦用户再次返回摄像头的视野，本发明的方法提供对该用户的重新认证。一旦确定了重新认证，显示和数据项被锁定，从而允许以如用户离开视野时的状态来立即访问设备。

[0032] 在通常的使用中，当利用该方法保护个人计算机的安全时，在设备上运行的应用软件不受影响，并且继续在设备上运行，尽管没有显示。不过，本发明的方法允许用户选择当设备变为锁定或解锁时设备影响的程度。因此，用户可以利用该方法确定来使得设备 1）锁定、2）解锁、3）登录、4）注销。设备的“锁定”提供了安全桌面，而不使用户断开文档或电子邮件服务器，并且不关闭在设备上运行的任何应用软件。当用户不在摄像头视野之内时，设备上的显示器、键盘和 / 或鼠标可能是失灵的。一旦用户回到视野，方法提供了重新认证。一旦重新建立了这种安全，则设备的显示器能再次使用。因此，这个过程在用户位于摄像头的视野之外时，提供了维护个人计算机或其他设备安全的简单方式。因为使用了脸部生物特征并且连续地认证用户，当用户暂时或长时间离开工作站时，能让用户放心的是显示在设备上的数据和对网络的访问将是安全的。

[0033] 图 3 是示出如图 2 中需要措连的持续认证程序的流程图。持续认证过程是本发明的关键特征，因为其允许用户在进入摄像头的视野之后被容易地重新认证。当授权已认证的用户访问并且解锁设备（在 303）时，持续认证过程（在 300）开始（在 301）。使用生物特征重新认证或脸部特征跟踪程序来确定用户仍然存在于摄像头的视野中（在 305）。在保持系统解锁时，允许用户脸部的重新认证为最高等级的安全。相反地，通过跟踪已认证用户的脸部特征，脸部特征跟踪允许使用低 CPU 资源来达到商业安全性。在本文中参考图 5 讨论脸部特征跟踪和持续认证。

[0034] 如果已认证用户离开了摄像头的视野（在 307），开始可选的延时的锁定时器过

程(在 309)。将参考图 5 充分地描述延时的锁定定时器过程。在该过程结束之后,锁定设备(在 311)。如果用户进入摄像头视野(在 313),需要确定可选的快速解锁定时器是否已过期(在 315)。如果使用了快速解锁定时器,快速解锁定时器通常是短暂的,通常为 1-10 秒。如果快速解锁定时器没有过期,则用现存的任意脸部而不是特定的脸部识别来解锁设备(在 335)。如果快速锁定定时器已过期,设备恢复用于认证的连续的生物特征扫描(在 317)。重新启动用户改变定时器(在 319),并且确定来自摄像头的图像是否与存储在数据库中的矢量相匹配(在 321)。如果摄像头图像不匹配任何存储的图像,则确定用户改变定时器是否已过期(在 323)。如果没有过期,则过程在图像与数据库不匹配的位置继续匹配图像(在 321)。如果用户改变定时器已过期,则继续生物特征扫描和数据库匹配并且向当前用户请求他的或她的认证证书。如果存在匹配,开始自动化的数据库过程(在 329),其将在图 4 中更充分地描述。如果在用户输入他的或她的证书之前有数据库的匹配而用户改变定时器已过期时,执行自动化的数据库过程(在 329)。在自动化的数据库过程结束处,将认为用户已被认证。系统将或者解锁设备(在 335),或者可选地注销已锁定计算机的现有用户(在 337)。接着系统会自动地将新用户登录到用户的账号而不用任何另外的认证。

[0035] 如果开始图像不匹配数据库的任何一个(在 321),可以可选地提示用户另外的认证因子,诸如密码短语或其他类型的密码。如果对于另外的认证因子没有匹配,则继续不间断的生物特征扫描(在 317)。如果存在匹配,需要确定这个现存的已认证用户是否为刚才暂时地离开视野的那个用户。如果是现有的已认证用户,解锁设备(在 335)。如果不是现有的用户,设备可被配置为注销现有用户(在 337)并且开始首次的登录过程(在 301),在该点结束连续的认证程序(在 339)。

[0036] 图 4 是用于填充数据库的过程及其能用于提高数据库中矢量质量的返回定时器过程(在 400)的流程图。自动化的数据库是这样的过程:通过该过程在用户使用系统并且输入密码,或在用户改变定时器过期之后发生数据库匹配时,将会创建或更新系统数据库。虽然最初需要密码,当时自动化数据库的目的是允许通过实际使用而不是特定的登记过程来填充数据,在其中用户最终能停止使用密码认证并且通过使用脸部生物特征数据,能采用本发明的方法来进行认证。无论何时当需要花过长的时间来用于数据库匹配时,通过更新数据库,可以提高数据库的质量并且减少用于随后数据库匹配的时间量。这也适用于随时间推移用户脸部的各种物理改变,包括老化、镜头的改变、肤色(晒黑的)、相对于摄像头用户的头部位置、变化的摄像头特性,和包括照明的各种环境条件。返回定时器过程的目的是在实际的识别或认证事件的时间之前用一个或多个图像来更新数据库。这允许当用户初次访问设备时,系统能获得更高重量的紧密匹配用户头部位置的图像。

[0037] 当从摄像头接收到视频帧(在 403)时,开始自动化的数据库和返回定时器过程(在 401)。启动用户改变定时器(在 405)并且需要确定图像是否为脸部图像。如果不是脸部图像,程序返回到接收视频(在 403)。一旦检测到了脸部图像,将视频帧及其时间戳临时地存储在存储器中(在 409)。时间戳指示了由摄像头处理的脸部图像的实际时间。做出比较来确定该图像是否与数据库中的另一图像矢量相匹配。如果产生匹配,则认证用户(在 427)。如果没有产生匹配,需要确定用户改变定时器是否已过期(在 413)。如果用户改变定时器没有过期,则接着查看图像来确定其是否为脸部图像(在 407)。如果用户改变定时器已过期,则向用户请求用户的姓名和密码,密码短语等(在 415)。如果用户没有用正确的证书进行认

证(在 417),则再次查看图像来确定其是否为脸部图像(在 407)。如果认证了用户,则基于实际的认证时间减去返回定时器的值来从存储器获得图像(在 419)。因为在向用户请求输入他的或她的证书时,还在接收视频帧(在 403)并且继续进行数据库匹配(在 411),所以即使在用户输入他的或她的证书时,系统也可以做出匹配并且往下进行用户认证(在 407)。下一步确定的是用户是否在数据库中具有先前存在的图像。如果用户在数据库中不具有先前存在的图像,则为该用户创建新的数据库(在 423)。随后,一旦创建了新数据库或先前存在的图像是可用的,则将获得的图像添加到用户的数据库(在 425)。接着认证了用户(在 427)并且结束过程(在 429)。

[0038] 图 5 是示出了用于本发明的持续认证实施例的连续的脸部特征跟踪和延时的锁定过程(在 500)的流程图。作为连续的认证方法的脸部特征跟踪的优点大致在于地中央处理单元(CPU)负载和相对于摄像头的用户脸部位置的高容差性。因为在极短时间内能够锁定系统或启动系统注销,所以延时的锁定接收器允许用户设置多快锁定系统来匹配用户的使用需求。这个过程在启动认证(在 215)之后立刻运行,直到锁定设备或注销设备。如果该条件存在,如果有用户脸部的跟踪或任何的鼠标或键盘活动,系统将保持解锁。这是期望之中的,因为锁定 / 注销动作可能发生得太快。一旦不再检测到鼠标或键盘活动,则在锁定设备之前,本发明的方法提供了可选的预定时间段。如果用户的脸部返回到视野或如果在不活动定时器过期之前,重新启动了键盘 / 鼠标活动,则不会锁定设备并且重置该定时器。

[0039] 更具体地,当授权已认证的用户访问解锁的设备(在 503)时,开始过程(在 501)。从摄像头接收视频帧(505)并且将一个或多个跟踪点放置到用户脸部的显著特征上(在 507)。接着对跟踪点的数量进行计数(在 509)并且需要确定目前有多少个跟踪点。如果跟踪点符合最小阈值,则在已授权用户访问(在 503)并且设备保持解锁的情况下再次开始过程,。如果跟踪点的数量低于最小阈值,则启动延时的锁定定时器(在 513)。参考图 6 更充分地描述用于使用延时的锁定定时器的过程。下一步确定是否由任何鼠标,键盘或其他外围设备的活动(例如在触屏上的活动)。如果没有活动,则在已认证的用户正访问解锁的设备情况下再次开始过程(在 503)。如果在鼠标或键盘上有活动,则确定延时的锁定定时器是否已过期(在 519)。如果延时的锁定定时器没有过期,则重新开始过程(在 503)。如果延时的锁定定时器已过期,则锁定设备(在 529)并且结束过程(在 521)。

[0040] 图 6 示出了连续的生物特征的认证 & 延时的锁定流程图,其为如在图 5 示出的连续的脸部特征跟踪和延时的锁定过程 500 的可替换的实施例。虽然图 6 中描述的方法非常类似于图 5 中描述的跟踪特征,但是连续的生物特征的认证提供了理论上更好的安全性,因为其不断地重新确认用户。实际上,连续的脸部特征跟踪会如此快速地锁定系统以至于新用户很难在系统锁定之前替换现有用户。为连续的生物特征的认识是非常 CPU 密集型的,并且需要用户的脸部在摄像头前方进行更加一致的替换。这两个因子使得连续的生物特征认识在许多环境和设备中不太理想。可替换的实现将包括连续的生物特征认证和连续的脸部特征跟踪二者的组合,其中大多数时间执行脸部特征跟踪并且在周期性的间隔中运行生物特征认证。

[0041] 在图 6 中,使用了连续的生物特征认证和延时的锁定过程 600。当已授权用户访问解锁的设备(在 603)时,开始过程(在 601)。从摄像头接收视频帧(在 605)并且确定图像是否匹配已认证的用户。如果图像不匹配,则在用户继续访问解锁的设备的情况下,再次启动

过程(在603)。如果图像不与已认证用户的图像相匹配,则启动延时的锁定定时器(在609)并且确定是否有任何的鼠标或键盘活动(在611)。如果不存在活动并且延时的锁定定时器已过期(在613),则将锁定设备或注销设备(在615)并且程序将结束(在617)。如果没有活动(在611)并且延时的锁定定时器没有过期(在613),则再次启动设备(在603)。如果有活动(在611)或延时的锁定定时器没有过期(在613),则再次启动过程(在603)。

[0042] 图7是根据本发明的可替换的实施例示出的系统和本发明的方法的拓扑的框图,其中屏幕模式和/或手势模式和摄像头被用来向用户提供系统认证。首先,本领域的技术人员应认识到"容忍"因子是能容忍的那些类型的输入或因子,因为它们能被接受而不具有向电子设备提供安全访问的准确精度。换句话说,准确的匹配可能是不必要的,相反仅是以一些预定义的方式的相似匹配。因此,能选择和/或调整特定的因子从而使"准确的"因子意味着它们的匹配容忍性必须是准确的和/或大致精确的以便允许访问设备。将正确运行的容忍或准确因子的等级通常由软件的制造商选择的;但是,这些类型因子的组合允许为设备提供极大的安全性的方法并同时使用户易于使用和访问。

[0043] 系统700包括根据图1描述的每一个组件;但是,这个设备还包括连接到电子设备701或在电子设备701中使用的触屏709。虽然所示使用了分离的键盘703,但是本领域的技术人员将认识到键盘703也可以用软件形成虚拟键盘来集成到触屏709中,从而使键盘703和触屏709可以当作一个设备。如本文指出的,触屏709将结合摄像头711操作,所述摄像头711的输入由微处理器705控制和解释。这允许用户在触屏709中输入手势,所述手势与摄像头711结合使用来为设备提供用户认证。这些输入与存储在数据库713中的数据和其他信息相比较。该数据能通过使用比较器715来进行比较,所述比较器715用于向访问电子设备701提供操作访问的比较类型分析。如本文描述的,可选的跟踪特征717也能用来确保设备的用户保持为同一个人,而在安全上没有缺口和漏洞。

[0044] 图8是示出用于向用户提供使用屏幕模式/手势和脸部生物特征二者的电子设备的又一可替换的实施例的流程图。使用屏幕手势和脸部生物特征二者的认证过程(在800)包括启动初始"登录"过程(在801)的步骤,所述步骤801触发了一些外部事件需要用户来输入认证证书。接着显示认证屏幕(在803)并且摄像头接收了至少一个视频帧(在805),从而使用户能接着输入预定义的屏幕手势或其他安全因子(在807)。虽然在实践中,对用户而言一个或多个安全因子像是在其他的因子之前发生,但是本领域的技术任何将进一步认识到在本发明的方法中,这些因子不需要同时发生或以特定的顺序发生。实际上,因为启动摄像头的延迟,这个步骤可以首先发生,但这不是必要的。

[0045] 随后,需要确定由摄像头接收的脸部识别帧与云还是与本地数据相匹配(在809)。本领域的技术人员将认识到"云计算"意味着经由数字网络使用多个服务器计算机,使其看起来似乎是一个计算机。可以经由因特网等访问使用云计算的计算机。如果使用尝试的次数或其他数据超过了一些预定时间段或一些计数器(在811),则要求用户输入可替换的证书或取消请求(在815)。如果没超过计数器,则摄像头将被用于提供另外的视频帧(在805)。一旦输入了可替换的证书,则需要确定证书是否与存储在数据库中的那些证书相匹配(在817)。如果证书匹配,则执行自动化的数据库过程来更新存储在数据库中的图像和/或其他数据(在819)。如果证书不匹配,则摄像头被用于为认证提供另外的视频帧(在805)。

[0046] 当手势与云或本地数据库不匹配(在 813)时,则再次要求用户输入可替换的证书或取消请求(在 815)。如果新的证书不匹配,则在有来自摄像头至少一个新帧(在 805)的情况下,再次开始过程;但是,如果新证书不匹配,则对自动化的数据库执行更新来更新脸部生物特征(在 819)。但是,如果手势匹配(在 813),则认证了用户并且能将本地或基于云的证书放入到特定的应用用于授权访问和 / 或使用(在 821)。任何更新的生物特征脸部数据将被用于在个认证过程(在 821)中。因而,清除认证屏幕(在 823)并且过程结束(在 825)。

[0047] 在典型的使用中,智能电话或需要认证的任意设备上的用户访问设备或需要认证的应用。该认证通常需要用户名和密码的输入。通过使用嵌入式正面成像设备(例如,摄像头)获得脸部识别模板来进行软件认证。大约在同时,提示用户输入其先前登记的手势。将脸部和手势与登记用户先前登记的模板的数据库进行比较。通过在几乎同时进行生物特征脸部数据和手势的比较,减小了每个因子的匹配容差,而不会降低安全的可靠性。因为极大地减少了通常将导致脸部识别或手势识别可信度降低以及通常会引起真实用户被不期望地错误拒绝的情况,所以这大大地改善了用户体验。

[0048] 本领域的技术人员可进一步认识到手势和生物特征信息的多种不同变型(例如,准确 / 容忍因子以及多个容忍因子)可以包括但不限于:

[0049] 准确因子和容忍因子

[0050] 密码和脸部

[0051] 密码和手势

[0052] 密码和模式

[0053] 密码和指纹

[0054] 个人身份号码和脸部

[0055] 个人身份号码和声音

[0056] 多个容忍因子

[0057] 脸部和手势

[0058] 脸部和部分密码(减少用于接受的密码字符的数目)

[0059] 脸部和模式

[0060] 脸部和指纹

[0061] 脸部和声音

[0062] 脸部、声音和手势

[0063] 脸部和形状

[0064] 形状和手势

[0065] 根据本发明的各种实施例,代替使用分配的登录名和密码,如本文描述的方法利用用户脸部的唯一的、单独的特征结合个人身份号码、手势(用户手指以其选择的模式在触摸屏上的活动)或者显示的符号、形状或其它标记的组合,来验证身份并提供安全且方便的访问。不仅该新方法提供了容易的访问,而且本文所描述的实施例解决了以容易、输入快速和无压力的方式保证双因子认证的问题。

[0066] 因此,本发明还能够提供个性化的、基于云的密码保险箱的、方便且通用的"单点登录"(一次登录多个应用和设备)。如本文所描述的,用户已知并键入具有许多字母、数字、形状或其它标记的密码来获得访问。从任何设备存储在保险箱中的密码在任何地方和在任

何其它设备上都立刻可得，并且可以缓存在本地设备上。该基于云的存储的优点在于所有的信息在被使用之前总是加密的。本发明的实施例还包括用于Windows、iOS、Android和其它操作系统设备的多平台支持。此外，密码还可以被存储在云中央并且被完全地加密。该布置的另一优点在于设备（电话、计算机、平板电脑等）可以被损坏、丢失或者重装，但是数据库将保持对认证用户的可访问。接着，本发明的方案允许多个用户安全地且彼此分离地共享单个移动设备。每个用户具有自己的私有密码内存存储区域或者仅通过个人唯一的脸部和手势可用的“保险箱”。

[0067] 因为PC具有减少的移动性并且通常仅用于受限数量的位置处，所以这种类型的条件允许用于识别匹配要求的更不容忍的设定。在这种设定下，PC通常具有非常低的错误报对率，在106错误报对／访问企图中仅仅为大约6.3。因此，在PC环境下，在学习的短暂时期之后，获得好的识别率的同时能维持高的准确性。然而，典型的PC环境是相对于照明和对脸部的观察面相对控制的。这并不适用于移动设备的情况，其中由于移动设备在照明和脸部的摄像头角度／脸部距摄像头的距离方面具有较高的差异，所以照明和手持移动设备对脸部的观察总是在显著地变化。为了在该变化环境下维持非常高的识别率，匹配容差必须稍微放松以便提供优良的识别率。不幸地是，放松容差还增加了不正确识别的可能性。即使是临时用户也不会容忍较高的错误识别率以及会导致对其私有数据的未认证访问。

[0068] 利用次级因子，例如当脸部被识别时的模式，指数级地增加了认证准确性，从而同时输入模式／个人身份号码以及脸部识别是非常快速、自然和方便的。这允许本发明实施脸部识别匹配容差值，其提供在变化的照明情况以及各种脸部角度下的优良识别，同时提高整体的认证准确性超过大部分认证方案。利用脸部识别和手势，可以最小化该两者的弱势。在脸部识别的情况下，手势防止照片或视频攻击，而脸部防止另一认证用户简单地观察和重复手势。因此，成功的“涂抹攻击”在没有脸部的情况下本质上不能进行访问。成功的“重播攻击”（照片／视频）而不利用手势也不能进行访问。具有多个因子也有助于最小化社交工程。当具有所有形式的安全／秘密时，对用户的个人了解会增加获得未经认证的访问的速度。要求多个独立类型的信息减小了任意单独条个人了解将是足够的这种可能性。

[0069] 图9A和图9B示出了展示动态手势布置的特征的触摸屏。图9A示出了当绘画区域保持在相同或一致位置时在触摸屏表面上留下的手指涂抹或残余的外观。因为该残余的模式，残余可能允许未认证的人员观察到给定的用户手势，降低了该因子的安全性。图9B示出了动态手势布置的使用，即当每次需要手势时，本发明的方法仔细地移动在触摸屏显示器上手势进入点的布置。显示器上的数据进入区域能够动态地移动和／或沿显示器上的任意方向歪斜，例如向上、向下、向侧边或沿对角线。该过程允许重叠油迹，这大大减小了认证人员能够推断手势的可能性。这消除了模式安全的共同弱点，即设备屏幕上的来自指油的油脂痕迹或其它残余能暗示或显示为用于手势或手指移动模式。

[0070] 图10示出了根据本发明的多个实施例实施的结合永久计算机可读介质使用的认证过程的流程图。认证过程1000开始于：用直播视频和在触摸屏显示器的数据输入或“手势”区域内的消息提示用户（在1001）。确定摄像头安置定时器是否过期（在1003）。如果没有，则该过程继续直到摄像头为捕捉一个或多个图像而充分静止达预订时间段。一旦定时器已经过期，那么用户的图像被捕捉到并在电子设备的触摸屏上转移给用户（在1005）。另外，可以向用户显示“开始扫描”动画以用于提供视频认证捕捉的通知，同时还可以在屏幕

上显示其它各种指标。为了捕捉预定数目的像素或帧，增加重试计数器，并将图像发送到用于评价的预定位置。

[0071] 之后，确定用户是否无效，也公知为“不良用户”（在 1007）。如果用户为无效的或者不良的（在 1009），那么显示器将通知用户需要初始“建立”或对系统软件进行编程（在 1009）。在这种情况下，用户通向次级建立步骤（在 1011）。然而，如果用户不是无效的，那么该过程确定是否检测用户的脸部（在 1013）。如果检测了，则保存脸部图像以用于稍后的学习步骤（在 1015），并且通过比较该脸部与本地存储或在云数据库中的数据以确定脸部是否经认证（在 1017）。如果脸部经认证，则过程继续以确定是否已经输入第二因子（在 1039）。如在本文中描述的，“第二因子”是手势或者是本文所描述的在触摸显示器上显示的符号组合的输入。然而，如果脸部未经认证（在 1017），则系统确定是否已经超过重试计数（在 1019）。如果未超过重试计数，则系统通知用户其未被识别（在 1037）并且通过提示用户再次开始过程（在 1001）。

[0072] 如果超过重试计数（在 1019），则系统确定是否保存了图像以用于稍后的学习步骤（在 1035）。如果保存了图像，则提醒用户输入用于学习用户脸部的云密码。之后，处理并存储用户的脸部图像（在 1036）。该过程将重试（在 1038）并输入清除状态（在 1044），或者如果输入了有效密码（在 1040），则保存图像以用于过程的系统“学习”步骤（在 1042）。确定有效用户认证（在 1029），从而授权用户访问电子设备（在 1031）。如果未保存图像（在 1035），则这将触发网络错误或者网络超时信息（在 1023），并且取消用户脸部认证处理步骤。之后，提示用户输入密码覆写（在 1025）。一旦输入并确认为有效密码（在 1027），可以发布有效认证命令（在 1029），并且授权用户访问电子设备（在 1031）。

[0073] 如此处需要注意的，一旦发生了脸部认证（在 1017），则进行第二确认用户是否已经输入了第二因子（在 1039）。第二因子可以包括但不限于屏幕手势、密码、显示符号的输入及其各种组合。如果第二因子是无效的（在 1041），则提示用户重新输入个人身份号码的手势（在 1043），并且该过程再次开始（在 1039）。然而，一旦第二因子是有效的（在 1041），则向用户显示批准或确认（在 1045），并且用户认证证书是有效的，从而授权他们访问电子设备（在 1031）。

[0074] 因此，如在密码覆写过程（在 1025）中所描述的，本发明的方法提供“回退”访问操作，从而在不能发生“标准”认证的情况下（例如，如果由于极端照明条件而不能进行脸部识别），单个的或者多因子的覆写是可以的。可以设置用于该覆写和每个因子的复杂要求以满足期望的安全目标。覆写选项包括但不限于以下输入：个人身份号码（PIN）；屏幕手势和 PIN；复杂密码（字母、数据和 / 或符号）；或者屏幕手势和复杂密码。

[0075] 有时在云中存储敏感信息会引起关注，因此仔细考虑通常是必要的，这是因为信息的未认证破坏对于系统操作而言是不利的。根据本发明的另一方案，可以利用具有固定块大小、重复计数和至少 128 位密钥的 Rijndael 对称算法，在云服务器和 / 或本地电子设备上对证书进行加密。该加密技术通常超过用于政府和财务数据的标准。利用对每个用户唯一的加密密钥，将网站证书加密为“数据二进制大对象（data blob）”。因此，在一个用户的账户被危害的不可能的情况下，由于除了用户外的其它方不会知道加密密钥或密码，所以不能将密钥用于访问其他用户的数据。由于该关键信息能保持未知的，所以总是推荐在当地备份证书数据库。由于从云恢复密码是不可能的，所以从不以未加密的状态传输数据。

实际上，直到在使用前不存在未加密状态。在该配置下，电子设备（电话、平板电脑、膝上电脑等）是简单的或者是“哑的”客户端，在其上通常并未本地存储数据。这意味着即使设备被盗，不管黑客花费多少努力，密码也不可能物理地显现。有限时间本地缓存是可选择地可用的，从而本发明能够允许管理员在必要时脱离网络而操作，同时能最小化风险。

[0076] 因此，本发明的系统和方法提供对个人计算机或者要求安全性的其它电子设备的快速、简单和安全访问。本发明在认证过程中结合使用屏幕手势和生物特征安全。通过结合在几乎同时分析的至少两种因子，能够降低容忍因子要求的容差匹配，而不降低电子设备的整体安全准确性。结合生物特征技术的该级别的安全性意味着，本发明唯一地提供利用多个平台可获得的基于云的安全证书快速、准确登录到设备、网站和 app，以及个性化访问设备，而无需例如 Android 和 iOS 的用户账户。结合本发明的实施例使用的成像是照明容忍的，对不想要的图像提供非常强的照片和视频拒绝。

[0077] 虽然已经示出并描述了本发明的优选实施例，但是清楚的是本发明并不限于此。在不背离所附权利要求限定的本发明的精神和范围的情况下，对本领域技术人员而言可以想到多种修改、变化、变型、替换和等价。如本文所使用的，术语“包括”、“包括有”或者其任何其它变型意图覆盖非排他的包含物，从而过程、方法、物品或包括一列元件的设备不仅包括那些元件，还可以包括未明确列出的或这种过程、方法、物品或设备所固有的其它元件。

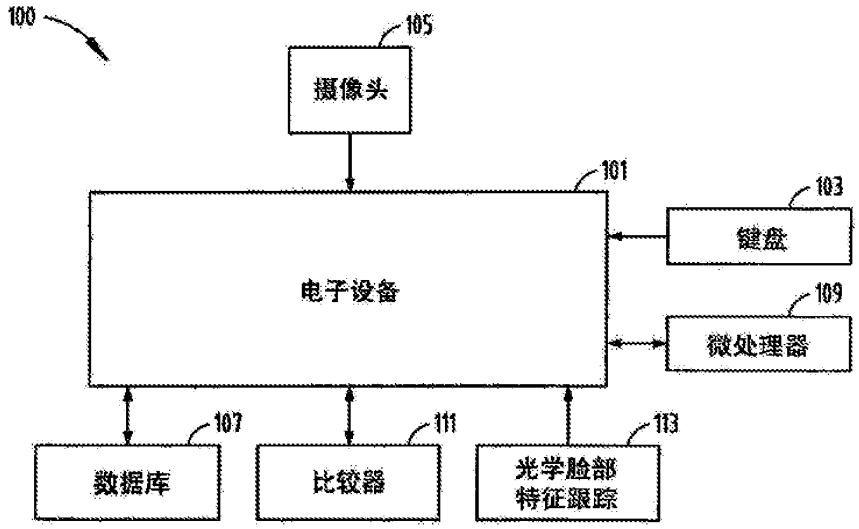

100
105
摄像头
101
103
键盘
电子设备
109
微处理器
107
111
113
数据库
比较器
光学脸部
特征跟踪

图 1

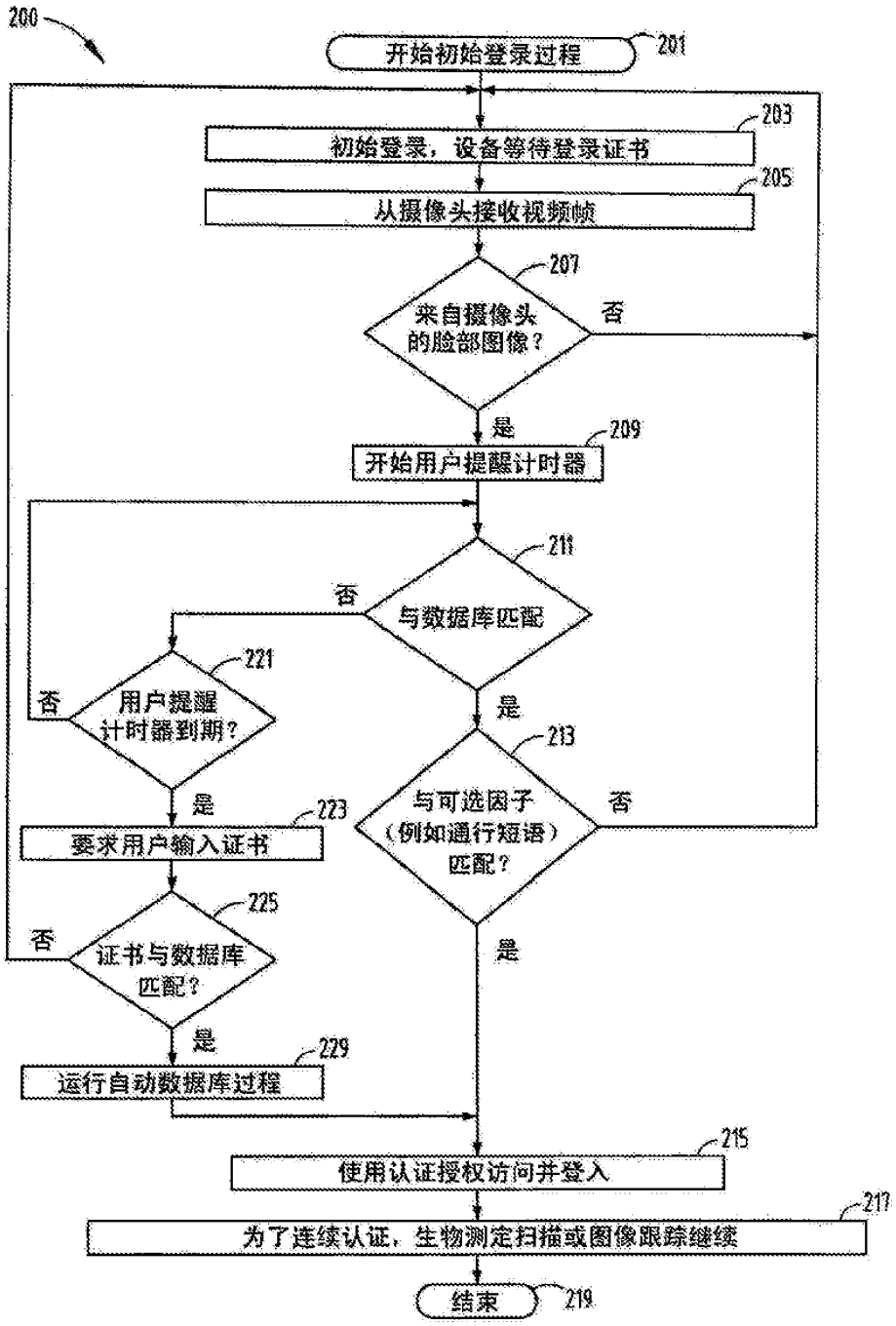

200
开始初始登录过程
201
初始登录，设备等待登录证书
203
从摄像头接收视频帧
205
来自摄像头的脸部图像？
207
否
是
开始用户提醒计时器
209
与数据库匹配
211
否
是
用户提醒计时器到期？
221
否
是
与可选因子（例如通行短语）匹配？
213
否
是
要求用户输入证书
223
证书与数据库匹配？
225
否
是
运行自动数据库过程
229
使用认证授权访问并登入
215
为了连续认证，生物测定扫描或图像跟踪继续
217
结束
219

图 2

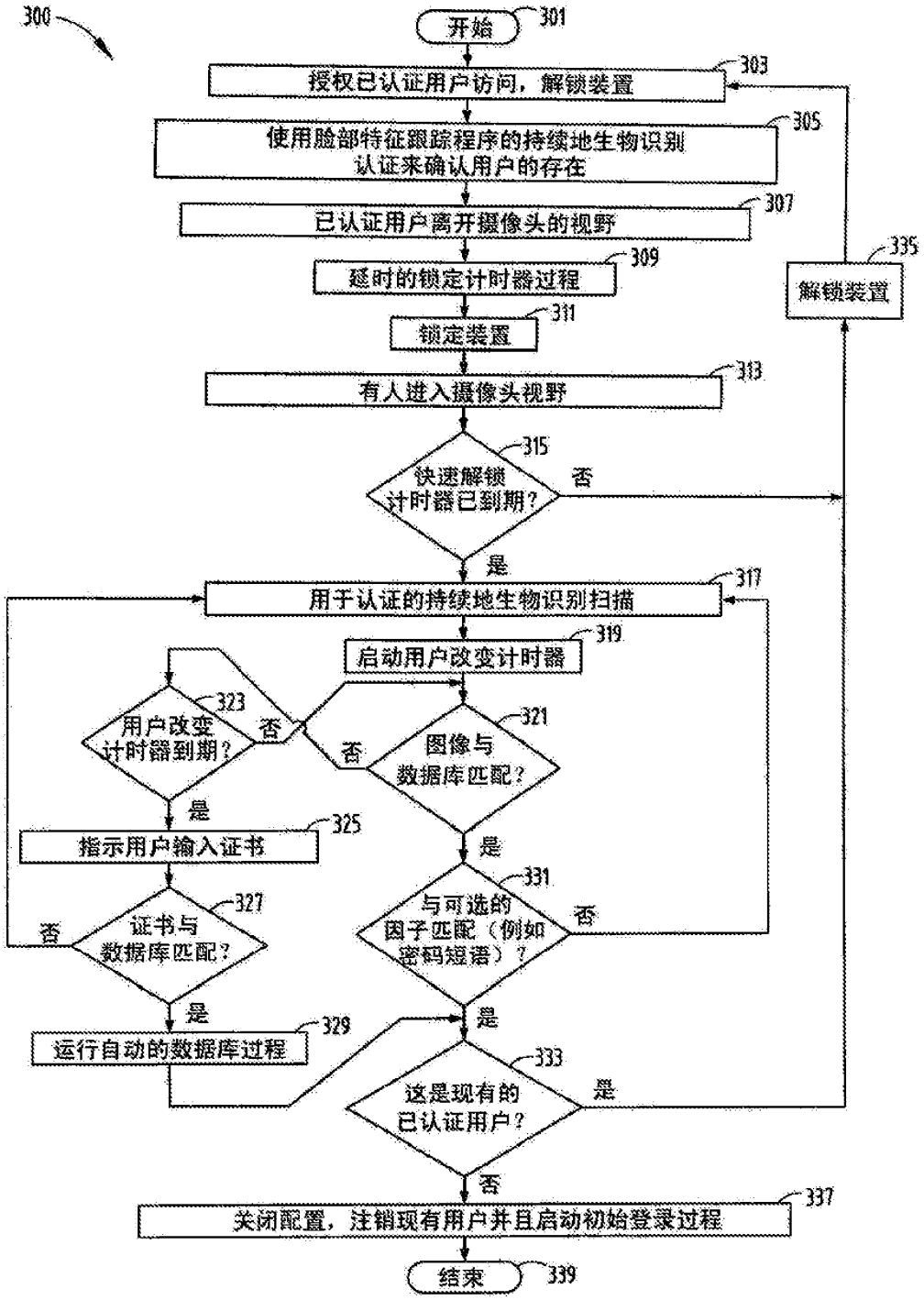

300
开始
301
授权已认证用户访问，解锁装置
303
使用脸部特征跟踪程序的持续地生物识别认证来确认用户的存在
305
已认证用户离开摄像头的视野
307
延时的锁定计时器过程
309
锁定装置
311
有人进入摄像头视野
313
快速解锁计时器已到期？
315
否
是
用于认证的持续地生物识别扫描
317
启动用户改变计时器
319
用户改变计时器到期？
323
否
图像与数据库匹配？
321
否
是
指示用户输入证书
325
是
证书与数据库匹配？
327
否
是
与可选的因子匹配（例如密码短语）？
331
否
是
运行自动的数据库过程
329
这是现有的已认证用户？
333
是
否
解锁装置
335
关闭配置，注销现有用户并且启动初始登录过程
337
结束
339

图 3

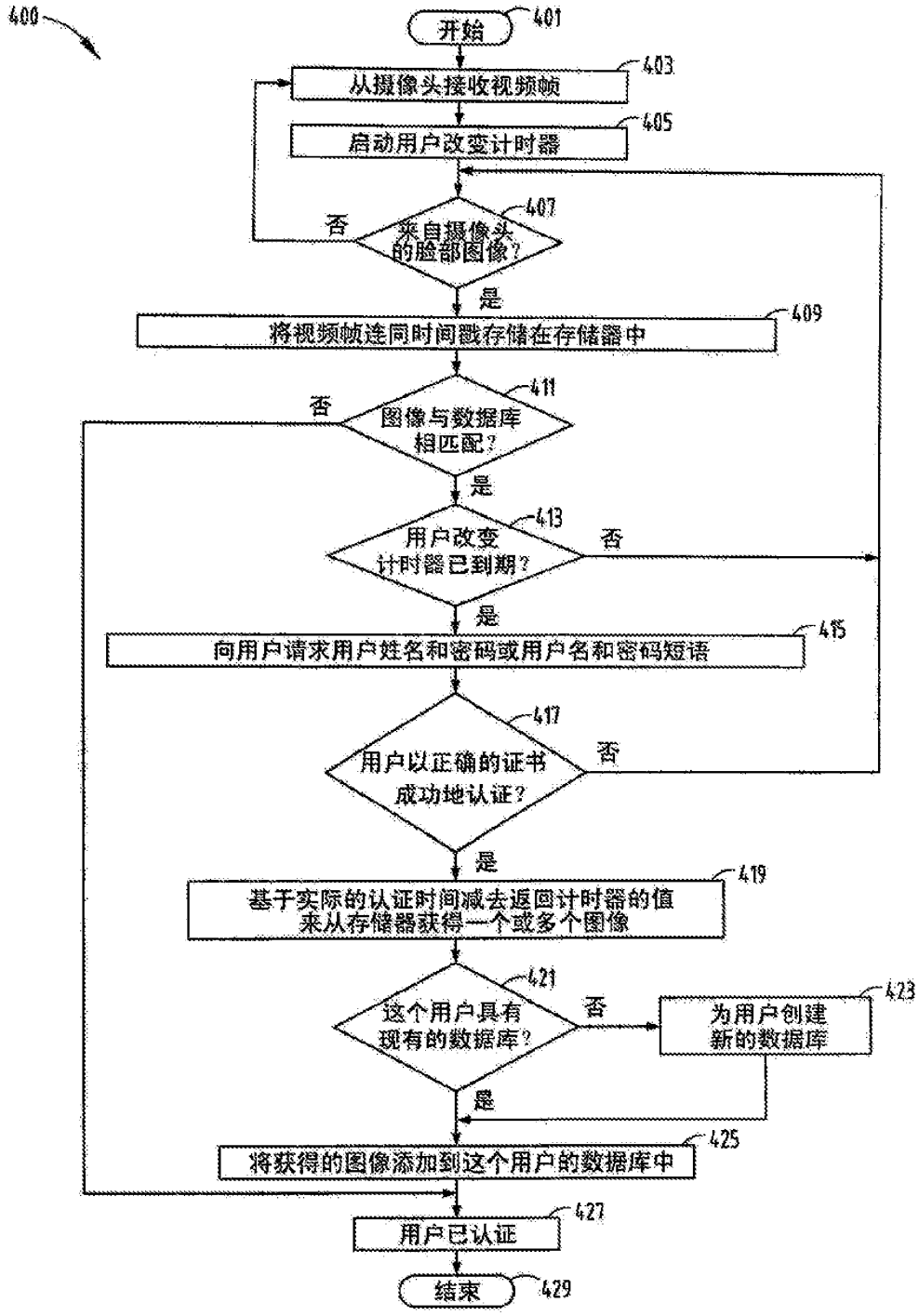

400
开始
401
从摄像头接收视频帧
403
启动用户改变计时器
405
来自摄像头的脸部图像?
407
否
是
将视频帧连同时间戳存储在存储器中
409
图像与数据库相匹配?
411
否
是
用户改变计时器已到期?
413
否
是
向用户请求用户姓名和密码或用户名和密码短语
415
用户以正确的证书成功地认证?
417
否
是
基于实际的认证时间减去返回计时器的值来从存储器获得一个或多个图像
419
这个用户具有现有的数据库?
421
否
为用户创建新的数据库
423
是
将获得的图像添加到这个用户的数据库中
425
用户已认证
427
结束
429

图 4

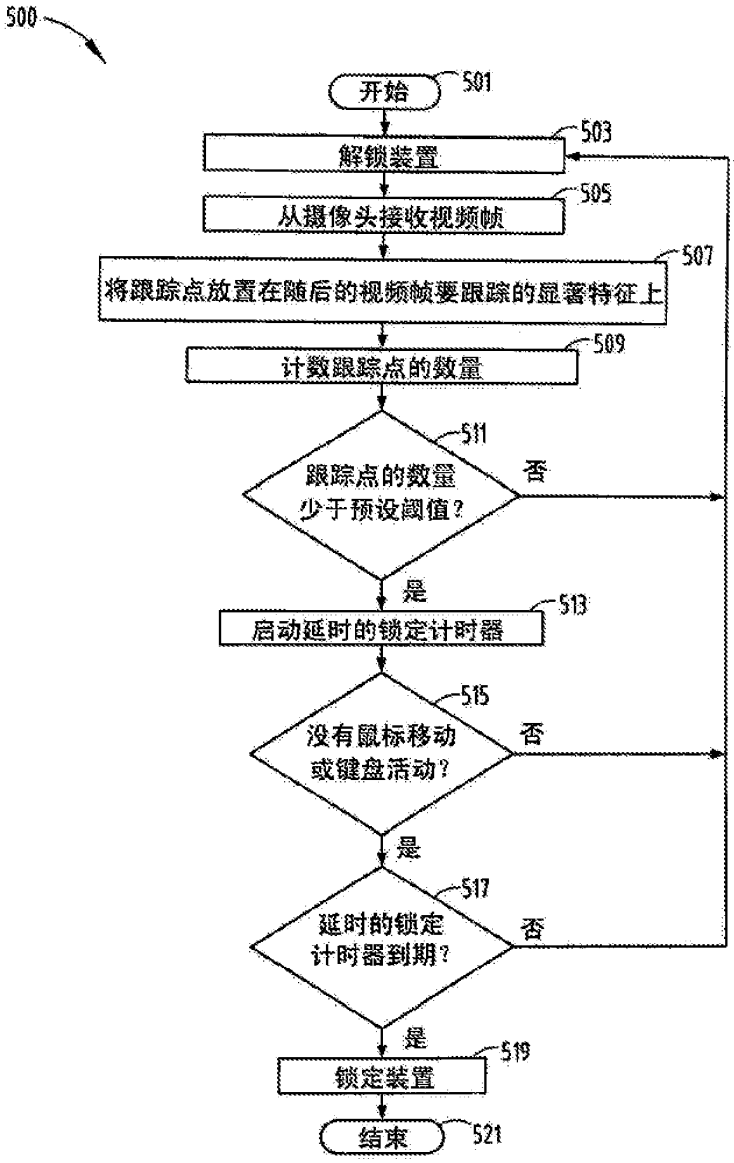

500
开始
501
解锁装置
503
从摄像头接收视频帧
505
将跟踪点放置在随后的视频帧要跟踪的显著特征上
507
计数跟踪点的数量
509
跟踪点的数量
少于预设阈值?
511
否
是
启动延时的锁定计时器
513
没有鼠标移动
或键盘活动?
515
否
是
延时的锁定
计时器到期?
517
否
是
锁定装置
519
结束
521

图 5

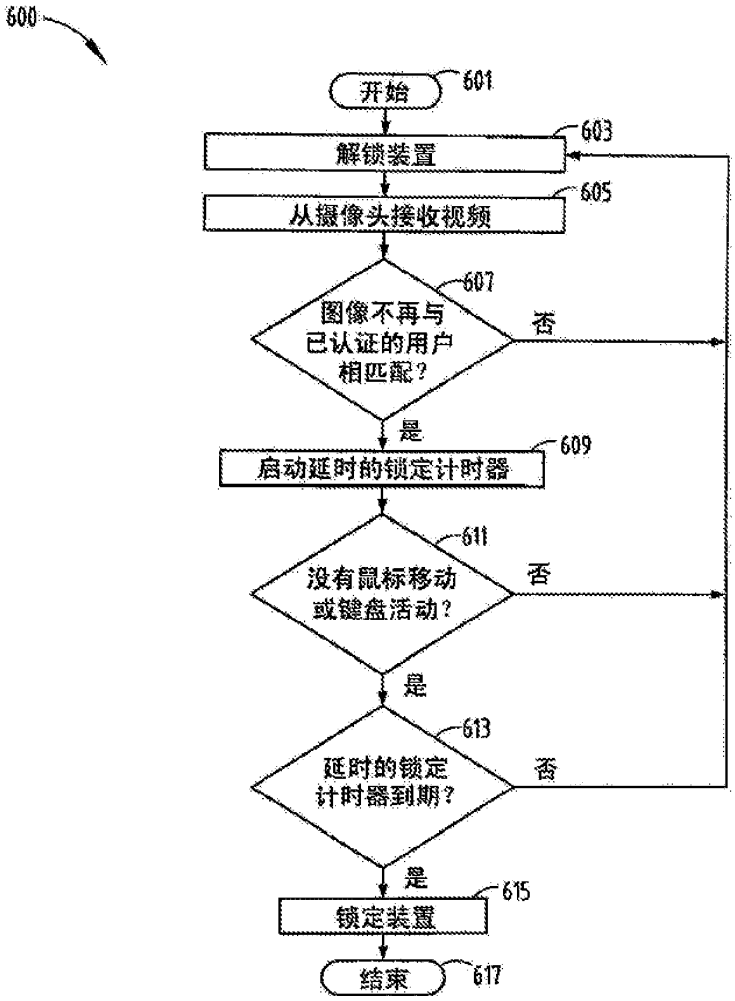

600
开始
601
解锁装置
603
从摄像头接收视频
605
图像不再与已认证的用户相匹配?
607
否
是
启动延时的锁定计时器
609
没有鼠标移动或键盘活动?
611
否
是
延时的锁定计时器到期?
613
否
是
锁定装置
615
结束
617

图 6

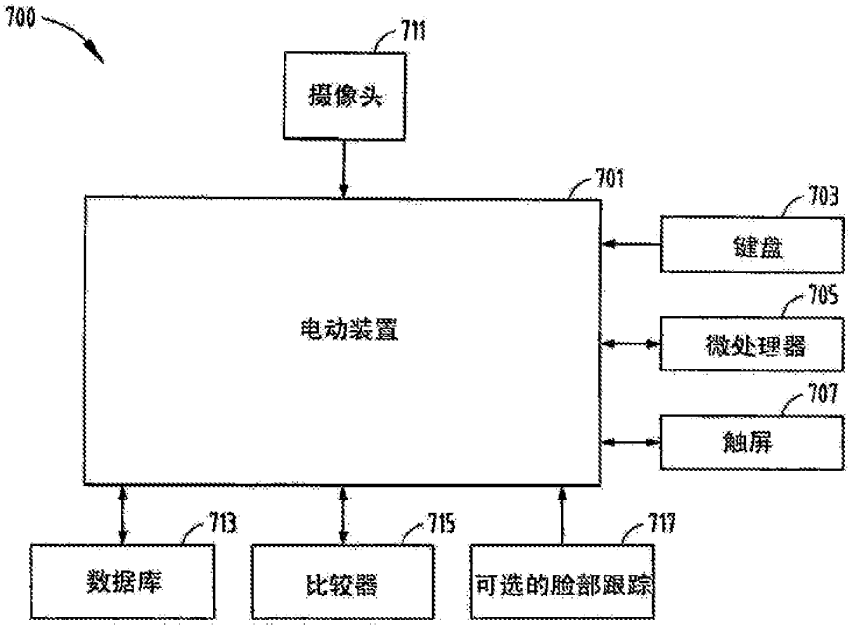

700
711
摄像头
701
703
键盘
电动装置
705
微处理器
707
触屏
713
715
717
数据库
比较器
可选的脸部跟踪

图 7

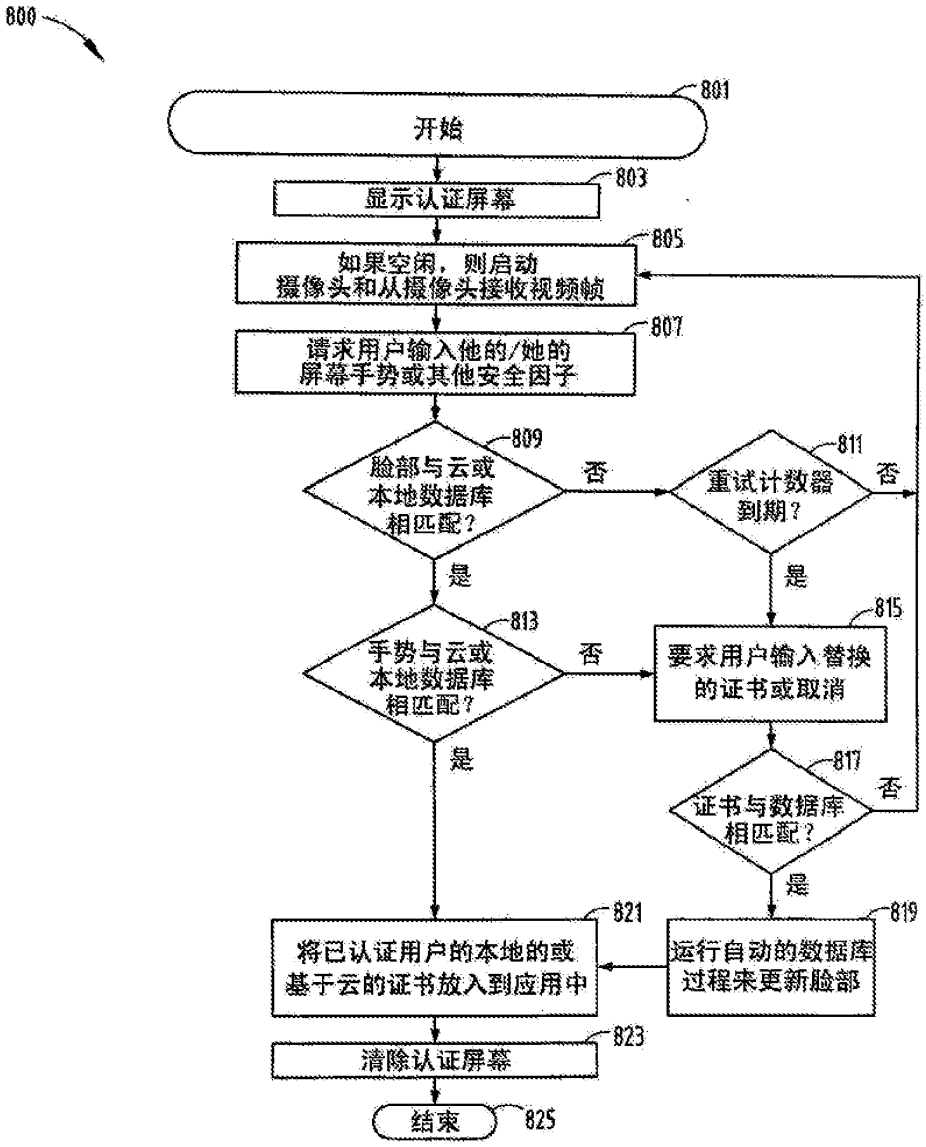

800
801
开始
803
显示认证屏幕
805
如果空闲，则启动
摄像头和从摄像头接收视频帧
807
请求用户输入他的/她的
屏幕手势或其他安全因子
809
脸部与云或
本地数据库
相匹配？
否
811
重试计数器
到期？
否
是
是
813
手势与云或
本地数据库
相匹配？
否
815
要求用户输入替换
的证书或取消
是
817
证书与数据库
相匹配？
否
是
821
将已认证用户的本地的或
基于云的证书放入到应用中
819
运行自动的数据库
过程来更新脸部
823
清除认证屏幕
结束
825

图 8

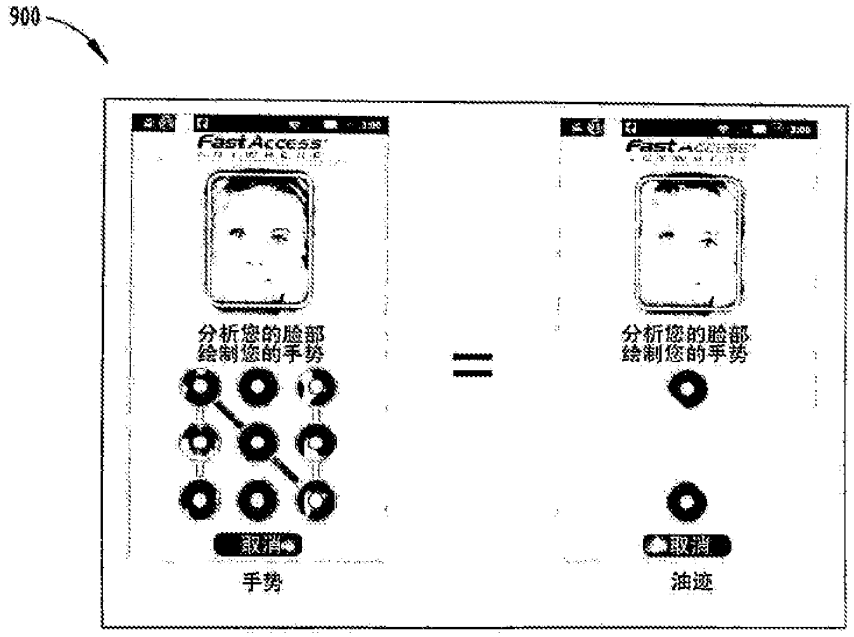

900
FastAccess
分析您的脸部
绘制您的手势
取消
手势
=
FastAccess
分析您的脸部
绘制您的手势
取消
油迹

图 9

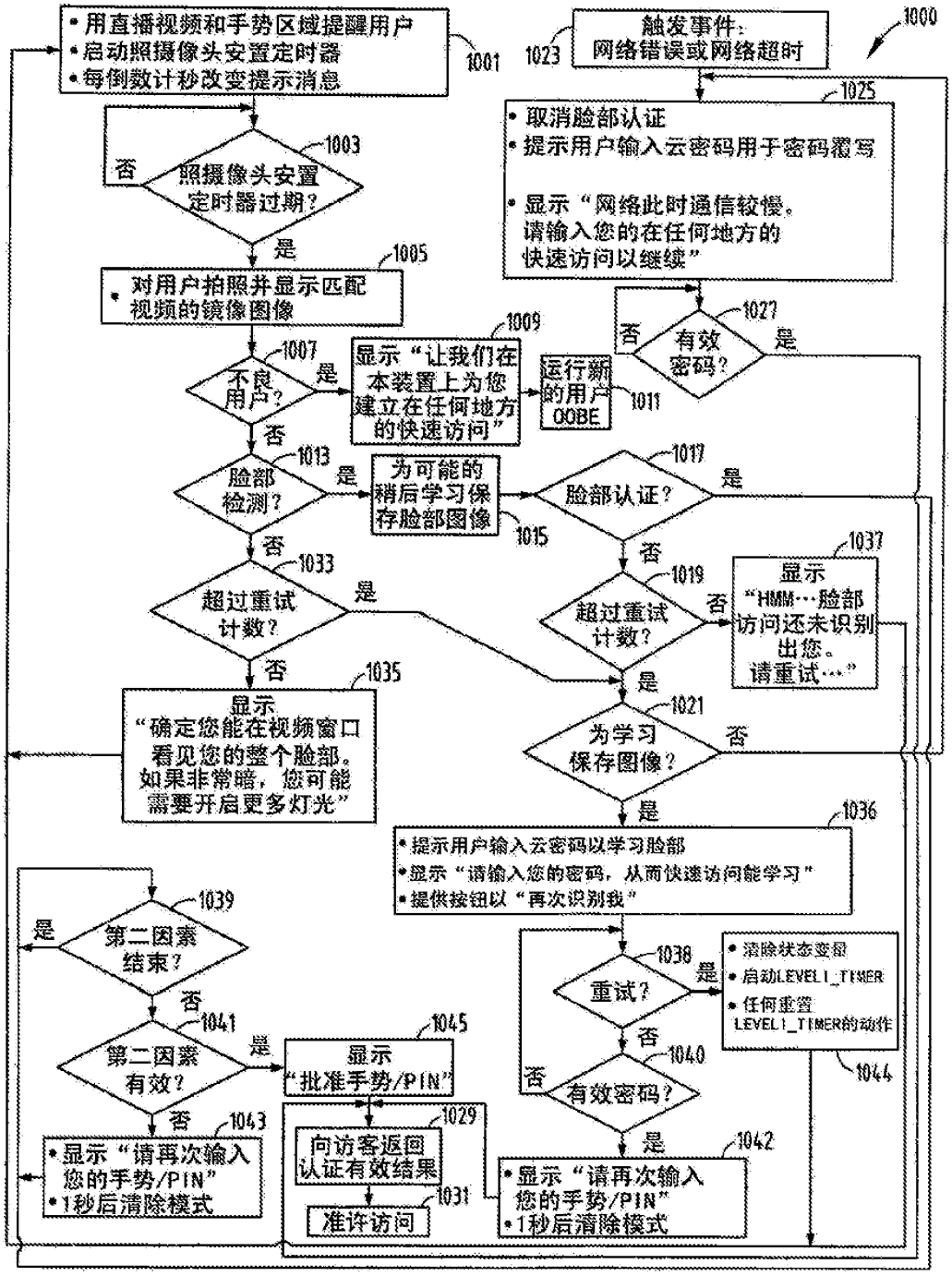

• 用直播视频和手势区域提醒用户
• 启动照摄像头安置定时器
• 每倒数计秒改变提示消息
1001
1000
触发事件：
网络错误或网络超时
1023
1025
• 取消脸部认证
• 提示用户输入云密码用于密码覆写
• 显示“网络此时通信较慢。
请输入您的在任何地方的
快速访问以继续”
照摄像头安置
定时器过期？
1003
否
是
对用户拍照并显示匹配
视频的镜像图像
1005
有效
密码？
1027
否
是
不良
用户？
1007
是
显示“让我们在
本装置上为您
建立在任何地方
的快速访问”
1009
运行新
的用户
OOBE
1011
否
脸部
检测？
1013
是
为可能的
稍后学习保
存脸部图像
1015
脸部认证？
1017
是
否
超过重试
计数？
1033
是
否
超过重试
计数？
1019
否
显示
“HMM…脸部
访问还未识别
出您。
请重试…”
1037
是
显示
“确定您能在视频窗口
看见您的整个脸部。
如果非常暗，您可能
需要开启更多灯光”
1035
为学习
保存图像？
1021
否
是
• 提示用户输入云密码以学习脸部
• 显示“请输入您的密码，从而快速访问能学习”
• 提供按钮以“再次识别我”
1036
第二因素
结束？
1039
是
否
重试？
1038
是
• 清除状态变量
• 启动LEVEL1_TIMER
• 任何重置
LEVEL1_TIMER的动作
1044
否
第二因素
有效？
1041
是
显示
“批准手势/PIN”
1045
否
有效密码？
1040
否
是
显示“请再次输入
您的手势/PIN”
• 1秒后清除模式
1043
向访客返回
认证有效结果
1029
准许访问
1031
显示“请再次输入
您的手势/PIN”
• 1秒后清除模式
1042

图 10

Electronic Acknowledgement Receipt

EFS ID:	24978816
Application Number:	14839505
International Application Number:	
Confirmation Number:	6236
Title of Invention:	Facial Recognition Authentication System Including Path Parameters
First Named Inventor/Applicant Name:	Kevin Alan Tussy
Customer Number:	32856
Filer:	Chad W. Miller
Filer Authorized By:	
Attorney Docket Number:	FACIAL.0012P
Receipt Date:	22-FEB-2016
Filing Date:	28-AUG-2015
Time Stamp:	17:42:01
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	CWMW10611TRANS.pdf	83972 7ef043b4d9d4997187e80eb982cb5f4eee8655b1	no	1

Warnings:	
Information:	

2	Information Disclosure Statement (IDS) Form (SB08)	CWMW10610PTO1449.pdf	87632 9fbf038f8544fc0761e1b58164361bab59e997e4	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Foreign Reference	REF1KR20130097581EngTrans.pdf	3067544 6c3f6c96388e39ab0fb4a6a253e0024751c22832	no	50
Warnings:					
Information:					
4	Foreign Reference	REF2CN103593594EngTrans.pdf	3475260 2f23a005183a2b46f9d7de2b4f3156b9e8ce8969	no	40
Warnings:					
Information:					
5	Non Patent Literature	REF3GirijaChettyAutoLipFeatExtract.pdf	1054434 c7dab8ab2c006809c9eb693cf737ab02bf7bf25e	no	6
Warnings:					
Information:					
		Total Files Size (in bytes):	7768842		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

FACIAL.0012P PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s)	:	Kevin Alan Tussy
App. No.	:	14/839,505
Filed	:	August 28, 2015
For	:	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS
Examiner	:	Cordelia P. K. Zecher

Group Art Unit: 2431

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Patent and Trademark Office via EFSWeb, on:

February 22, 2016
(Date)

/Chad W. Miller/
Chad W. Miller, Reg. No. 44,943

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Enclosed is form PTO-1449 listing two (2) U.S. references, copies of which are not required to be provided in accordance with 37 C.F.R. §1.98(e), two (2) foreign references and one (1) publication, copies of which are enclosed herewith . This Information Disclosure Statement is being filed before the mailing of the first Office Action on the merits, and as such, no fee is required in accordance with 37 C.F.R. §1.97(b)(3).

Respectfully submitted,

Dated: February 22, 2016

By: /Chad W. Miller/
Chad W. Miller
Attorney for Applicant
Weide & Miller, Ltd.
Registration No. 44,943
7251 W. Lake Mead Blvd., Suite 530
Las Vegas, NV 89128
Tel. (702) 382-4804 (Pacific Time)
cmiller@weidemiller.com

CWM-W-10611

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE (MODIFIED) PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. FACIAL.0012P	APPLICATION NO. 14/839,505
INFORMATION DISCLOSURE CITATION BY APPLICANT	INVENTOR(S) Kevin Alan Tussy	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE August 28, 2015	GROUP ART UNIT 2431

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPLICABLE)
		5,956,122	09/99	Doster			
		7,428,320	09/08	Northcott, et al.			
		2010/0310133	12/10	Mason, et al.			
		8,280,120	10/12	Hoyos, et al.			
		8,411, 909	04/13	Zhao, et al.			

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
							YES	NO

EXAMINER INITIAL	**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)	

EXAMINER	DATE CONSIDERED

***EXAMINER**: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

CWM-W-10485

Electronic Acknowledgement Receipt

EFS ID:	24609930
Application Number:	14839505
International Application Number:	
Confirmation Number:	6236
Title of Invention:	Facial Recognition Authentication System Including Path Parameters
First Named Inventor/Applicant Name:	Kevin Alan Tussy
Customer Number:	32856
Filer:	Chad W. Miller
Filer Authorized By:	
Attorney Docket Number:	FACIAL.0012P
Receipt Date:	13-JAN-2016
Filing Date:	28-AUG-2015
Time Stamp:	20:39:51
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	CWMW10484TRANS.pdf	83778 a79816b86578b4c6f588b924e477dbad8e3e532c	no	1

Warnings:	
Information:	

2	Information Disclosure Statement (IDS) Form (SB08)	CWMW10485PTO1449.pdf	81972 67ca2c30cf7df762f41c0bf8ffc722cab37e94da	no	1

Warnings:	
Information:	
This is not an USPTO supplied IDS fillable form	
Total Files Size (in bytes):	165750

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

FACIAL.0012P PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s)	:	Kevin Alan Tussy
App. No.	:	14/839,505
Filed	:	August 28, 2015
For	:	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS
Examiner	:	Unknown

Group Art Unit: 2431

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Patent and Trademark Office via EFSWeb, on:

January 13, 2016
(Date)

/Chad W. Miller/
Chad W. Miller, Reg. No. 44,943

INFORMATION DISCLOSURE STATEMENT

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Enclosed is form PTO-1449 listing five (5) U.S. references, copies of which are not required to be provided in accordance with 37 C.F.R. §1.98(e). This Information Disclosure Statement is being filed before the mailing of the first Office Action on the merits, and as such, no fee is required in accordance with 37 C.F.R. §1.97(b)(3).

Respectfully submitted,

Dated: January 13, 2016

By: /Chad W. Miller/
Chad W. Miller
Attorney for Applicant
Weide & Miller, Ltd.
Registration No. 44,943
7251 W. Lake Mead Blvd., Suite 530
Las Vegas, NV 89128
Tel. (702) 382-4804 (Pacific Time)
cmiller@weidemiller.com

CWM-W-10484

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/839,505

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	21 minus 20 =	* 1	x 40 =	40	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	770		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)	OR	RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/839,505	08/28/2015	2431	770	FACIAL.0012P	21	3

CONFIRMATION NO. 6236

FILING RECEIPT

32856
WEIDE & MILLER, LTD.
7251 W. LAKE MEAD BLVD.
SUITE 530
LAS VEGAS, NV 89128

OC000000077399525

Date Mailed: 09/14/2015

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Kevin Alan Tussy, Las Vegas, NV;

Applicant(s)

Kevin Alan Tussy, Las Vegas, NV;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This appln claims benefit of 62/043,224 08/28/2014

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

If Required, Foreign Filing License Granted: 09/11/2015

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/839,505**

Projected Publication Date: 03/03/2016

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****

Title

Facial Recognition Authentication System Including Path Parameters

Preliminary Class

726

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	FACIAL.0012P
	Application Number	
Title of Invention	Facial Recognition Authentication System Including Path Parameters	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Kevin	Alan	Tussy	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Las Vegas	State/Province	NV	Country of Residence i	US

Mailing Address of Inventor:

Address 1	1707 Village Center Circle, Suite 200		
Address 2			
City	Las Vegas	State/Province	NV
Postal Code	89134	Country i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	000032856		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	Facial Recognition Authentication System Including Path Parameters		
Attorney Docket Number	FACIAL.0012P	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	14	Suggested Figure for Publication (if any)	

Filing By Reference :

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	FACIAL.0012P
	Application Number	
Title of Invention	Facial Recognition Authentication System Including Path Parameters	

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	000032856		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Claims benefit of provisional	62/043224	2014-08-28

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	FACIAL.0012P
	Application Number	
Title of Invention	Facial Recognition Authentication System Including Path Parameters	

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) [i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country [i]	Filing Date (YYYY-MM-DD)	Access Code [i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☒ Authorization to Permit Access to the Instant Application by the Participating Offices

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	FACIAL.0012P
	Application Number	
Title of Invention	Facial Recognition Authentication System Including Path Parameters	

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◯ Assignee	◯ Legal Representative under 35 U.S.C. 117	◯ Joint Inventor
◯ Person to whom the inventor is obligated to assign.	◯ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	FACIAL.0012P
	Application Number	
Title of Invention	Facial Recognition Authentication System Including Path Parameters	

Mailing Address Information:			
Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	FACIAL.0012P
	Application Number	
Title of Invention	Facial Recognition Authentication System Including Path Parameters	

Signature:

Remove

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications					
Signature	/Brian G. Prince/			Date (YYYY-MM-DD)	2015-08-28
First Name	Brian	Last Name	Prince	Registration Number	70569

Additional Signature may be generated within this form by selecting the Add button. Add

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [■] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: KEVIN ALAN TUSSY Date (Optional) : _____

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS

INVENTOR

KEVIN ALAN TUSSY

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Application No. 62/043,224 which was filed August 28, 2014; U.S. Provisional Application No. 62/054,847 which was filed on September 24, 2014; U.S. Provisional Application No. 62/064,415 which was filed on October 15, 2014; U.S. Provisional Application No. 62/085,963 which was filed on December 1, 2014; U.S. Provisional Application No. 62/101,317 which was filed on January 8, 2015; U.S. Provisional Application No. 62/139,558 which was filed on March 27, 2015; and U.S. Provisional Application No. 62/188,584 which was filed on July 3, 2015. The contents of each of the above applications are incorporated by reference.

BACKGROUND

1. Field

[0002] The disclosed embodiments relate to biometric security. More specifically, the disclosed embodiments relate to a facial recognition authentication systems.

2. Related Art

[0003] With the growth of personal electronic devices that may be used to access a number of user accounts, and the increasing threat of identity theft and other security issues, there is a growing need for ways to securely access user accounts via electronic devices. Account holders are thus often required to have longer passwords that meet various criteria such as using a mixture of capital and lowercase letters, numbers, and other symbols. With smaller electronic devices, such as smart phones, smart watches, "Internet of Things" ("IoT") devices and the like, it may become cumbersome to attempt to type such long passwords into the device each time access to the account is desired. In some instances, users may even decide to deactivate such cumbersome security measures due to their inconvenience on their devices. Thus, users of such devices may prefer other methods of secure access to their user accounts.

[0004] One other such method may be through the use of biometrics. For example, an electronic device may have an optical reader that may scan a user's fingerprint to determine that the person requesting access to a device or an account is authorized. However, such fingerprint systems are often prohibitively expensive for use on a small electronic device, or are often considered unreliable and unsecure.

[0005] In addition, facial recognition is generally known and may be used in a variety of contexts. Two-dimensional facial recognition is commonly used to tag people in images on social networks or in photo editing software. Facial recognition software, however, has not been widely implemented on its own to securely authenticate users attempting to gain

access to an account because it not considered secure enough. For example, two dimensional facial recognition is considered unsecure because faces may be photographed or recorded, and then the resulting prints or video displays showing images of the user may be used to trick the system. Accordingly, there is a need for reliable, cost-effective, and convenient method to authenticate users attempting to log in to, for example, a user account.

SUMMARY

[0006] The disclosed embodiments have been developed in light of the above and aspects of the invention may include a method for enrolling and authenticating a user in an authentication system via a user's a mobile computing device. The user's device includes a camera and at least one movement detecting sensor, such as an accelerometer, magnetometer, and gyroscope.

[0007] In one embodiment, the user may enroll in the system by providing enrollment images of the user's face. The enrollment images are taken by the camera of the mobile device as the user moves the mobile device to different positions relative to the user's head. The user may thus obtain enrollment images showing the user's face from different angles and distances. The system may also utilize one or more movement sensors of a mobile device to determine an enrollment movement path that the phone takes during the imaging. At least one image is processed to detect the user's face within the image, and to obtain biometric information from the user's face in the image. The image processing may be done on the user's mobile device or at a remote device, such as an authentication server or a user account server. The enrollment information (the enrollment biometrics, movement, and other information) may be stored on the mobile device or remote device.

[0008] The system may then authenticate a user by the user providing at least one authentication image via the camera of the mobile device while the user moves the mobile device to different positions relative to the user's head. The authentication images are processed for face detection and facial biometric information. Path parameters are also

obtained during the imaging of the authentication images (authentication movement). The authentication information (authentication biometric, movement, and other information) is then compared with the enrollment information to determine whether the user should be authenticated or denied. Image processing and comparison may be conducted on the user's mobile device, or may be conducted remotely.

[0009] In some embodiments, multiple enrollment profiles may be created by a user to provide further security. For example, a user may create an enrollment wearing accessories such as a hat or glasses, or while making a funny face. In further embodiments, the user's enrollment information may be linked to a user email address, phone number, or other identifier.

[0010] The authentication system may include feedback displayed on the mobile device to aid a user in learning and authentication with the system. For instance, an accuracy meter may provide feedback on a match rate of the authentication biometrics or movement. A movement meter may provide feedback on the movement detected by the mobile device.

[0011] In some embodiments, the system may reward users who successfully utilize the authentication system or who otherwise take fraud preventing measures. Such rewards may include leaderboards, status levels, reward points, coupons or other offers, and the like. In some embodiments, the authentication system may be used to login to multiple accounts.

[0012] In addition to biometric and movement matching, some embodiments may also utilize banding detection, glare detection, and screen edge detection to further secure the system. In other embodiments, other user attributes may be detected and matched including users' gender, age, ethnicity, and the like.

[0013] The system may also provide gradual access to user account(s) when the user first sets up the authentication system. As the user successfully implements the system, authorization may be expanded. For example, during a time period as the user gets accustomed to the authentication system, lower transaction limits may be applied.

[0014] In some embodiments, the mobile device may show video feedback of what the user is imaging to aid the user to image his or her face during enrollment or authentication. The video feedback may be displayed on only a portion of the display screen of the mobile device. For example, the video feedback may be displayed in an upper portion of the display screen. The video feedback display may be position on a portion of the display screen that corresponds with a location of a front-facing camera of the mobile device.

[0015] To facilitate imaging in low-light, portions of the screen other than the video feedback may be displayed in a bright color, such as white. In some embodiments, and LED or infrared light may be used, and near infrared thermal imaging may be done with an infrared camera. The mobile device used for imaging may thus have multiple cameras for capture visible light and infrared images. The mobile device may also have multiple cameras (two or more) imaging in a single spectrum or multiple spectrum to provide

stereoscopic, three-dimensional images. In such an embodiment, the close-up frames (zoomed) may create the most differentiation as compared to images captured from a distance. In such an embodiment, the frames captured at a distance may be unnecessary.

[0016] In some embodiments, to provide added security, the mobile device may output objects, colors, or patterns on the display screen to be detected during the imaging. The predetermined object or pattern may be a unique one-dimensional or two-dimensional barcode. For example, a QR code (two-dimensional barcode) may be displayed on the screen and reflected off of the user's eye. If the QR code is detected in the image, then the person may be authenticated. In other embodiments, an object may move on the screen and the system may detect whether a user's eyes follow the movement.

[0017] In some embodiments, the system may provide prompts on a video feedback display to aid the user in moving the device relative to the user's head during enrollment and/or authentication. The prompts may include ovals or frames displayed on the display screen in which the user must place his or her face by moving the mobile device until his or her face is within the oval or frame. The prompts may preferably be of differing sizes and may also be centered on different positions of the screen. When an actual, three-dimensional person images himself or herself close up and far away, it has been found that the biometric results are different due to the fish-eye effect of the lens. Thus, a three-dimensional person may be validated when biometric results are different in the close-up and far away images. This also allows the user to have multiple biometric profiles for each of the distances.

[0018] In other embodiments, biometrics from images obtained between the close-up and far away images may be analyzed for incrementally different biometric results. In this manner, the morphing of the face from the far face to the warped close up face is captured and tracked. The incremental frames during an authentication may then be matched to frames captured at similar locations during enrollment along the motion path and compared to ensure that the expected similarities and difference are found. This results in a motion path and captured image and biometric data that can prove a three-dimensional person is presently being imaged. Thus, not only are the close-up and far away biometrics compared, but also biometric data obtained in between. The biometric data obtained in between must also correspond to a correct morphing speed along the motion path, greatly enhancing the security of the system.

[0019] The touch screen may be utilized in some embodiments. For example, the user may need to enter a swipe a particular code or pattern in addition to the authentication system described herein. The touchscreen may also detect a size and orientation of a user's finger, and whether or not a right hand or a left hand is used on the touch screen. Voice parameters may also be used as an added layer of security. The system may detect edge sharpness or other indicators to ensure that the obtained images are of sufficient quality for the authentication system.

[0020] When a camera has an autofocus, the autofocus may be controlled by the system to validate the presence of the actual, three-dimensional person. The autofocus may check that different features of the user or environment focus at different focal lengths. In other

embodiments, authentication images may be saved to review the person who attempted to authenticate with the system.

[0021] In some embodiments, the match thresholds required may be adapted over time. The system may thus account for changing biometrics due to age, weight gain/loss, environment, user experience, security level, or other factors. In further embodiments, the system may utilize image distortion prior to obtaining biometric information to further protect against fraudulent access.

[0022] The system may utilize any number or combination of the security features as security layers, as described herein. When authentication fails, the system may be configured so that it is unclear which security layer triggered the failure to preserve the integrity of the security system.

[0023] Other systems, methods, features and advantages of the invention will be or will become apparent to one with skill in the art upon examination of the following figures and detailed description. It is intended that all such additional systems, methods, features and advantages be included within this description, be within the scope of the invention, and be protected by the accompanying claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0024] The components in the figures are not necessarily to scale, emphasis instead being placed upon illustrating the principles of the invention. In the figures, like reference numerals designate corresponding parts throughout the different views.

[0025] Figure 1 illustrates an example environment of use of the facial recognition authentication system, according to one exemplary embodiment.

[0026] Figure 2 illustrates an example embodiment of a mobile device.

[0027] Figure 3 illustrates exemplary software modules that are part of the mobile device and server.

[0028] Figure 4 shows a method for performing facial recognition authentication according to one embodiment.

[0029] Figure 5 shows a method for enrolling a user in a facial recognition authentication system, according to one exemplary embodiment.

[0030] Figures 6A and 6B show an example of movement of a mobile device about a user's face according to one exemplary embodiment.

[0031] Figures 7A and 7B show an example of movement of a mobile device about a user's face according to one exemplary embodiment.

[0032] Figure 8 shows a method of providing authentication information in a facial recognition authentication system, according to one exemplary embodiment.

[0033] Figure 9 shows a method of verifying authentication credential in a facial recognition authentication system, according to one exemplary embodiment.

[0034] Figure 10 illustrates an exemplary display showing a graphical and numeric feedback in a facial recognition authentication system.

[0035] Figures 11A, 11B, and 11C illustrate exemplary video feedback displays corresponding to front-facing camera positions in a facial recognition authentication system.

[0036] Figure 12 shows an exemplary video display feedback of a facial recognition authentication system where edge pixels on the sides of the display are stretched horizontally.

[0037] Figures 13A and 13B illustrates exemplary screen displays with face alignment indicators shown as an oval to serve as a guide as the user moves the mobile device closer to or away from their face.

[0038] Figure 14 illustrates an exemplary mobile device display showing a graphical code entry interface with an imaging area.

[0039] Figure 15 illustrates an example mobile device display showing a numeric and graphical code entry interface with an imaging area.

DETAILED DESCRIPTION OF EMBODIMENTS

[0040] A system and method for providing secure and convenient facial recognition authentication will be described below. The system and method may be achieved without the need for additional expensive biometric readers or systems while offering enhanced security over conventional facial recognition systems.

Facial Recognition Authentication Environment

[0041] Figure 1 illustrates an example environment of use of the facial recognition authentication system described herein. This is but one possible environment of use and system. It is contemplated that, after reading the specification provided below in connection with the figures, one of ordinary skill in the art may arrive at different environments of use and configurations.

[0042] In this environment, a user 108 may have a mobile device 112 which may be used to access one or more of the user's accounts via authentication systems. A user 108 may have a mobile device 112 that is capable of capturing a picture of the user 108, such as an image of the user's face. The user may use a camera 114 on or connected to the mobile device 112 to capture an image or multiple images or video of himself or herself. The mobile device 112 may comprise any type of mobile device capable of capturing an image, either still or video, and performing processing of the image or communication over a network.

[0043] In this embodiment, the user 108 may carry and hold the mobile device 112 to capture the image. The user may also wear or hold any number of other devices. For, example, the user may wear a watch 130 containing one or more cameras 134 or biosensors disposed on the watch. The camera 134 may be configured to create an image from visible light as well as infrared light. The camera 134 may additionally or alternatively employ image intensification, active illumination, or thermal vision to obtain images in dark environments.

[0044] When pointed towards a user 108, the camera 134 may capture an image of the user's face. The camera 134 may be part of a module that may either include communication capability that communicates with either a mobile device 112, such as via Bluetooth®, NFC, or other format, or communication directly with a network 116 over a wired or wireless link 154. The watch 130 may include a screen on its face to allow the user to view information. If the camera module 134 communicates with the mobile device 112, the mobile device 134 may relay communications to the network 116. The mobile device 134 may be configured with more than one front facing camera 114 to provide for a 3D or stereoscopic view, or to obtain images across a different spectral ranges, such as near infrared and visible light.

[0045] The mobile device 112 is configured to wirelessly communicate over a network 116 with a remote server 120. The server 120 may communicate with one or more databases 124. The network 116 may be any type of network capable of communicating to and from the mobile device including but not limited to a LAN, WAN, PAN, or the

Internet. The mobile device 112 may communicate with the network via a wired or wireless connection, such as via Ethernet, WiFi, NFC, and the like. The server 120 may include any type of computing device capable of communicating with the mobile device 112. The server 120 and mobile device 112 are configured with a processor and memory and are configured to execute machine readable code or machine instructions stored in the memory.

[0046] The database 124, stored on mobile device or remote location as shown, may contain facial biometric information and authentication information of users 108 to identify the users 108 to allow access to associated user data based on one or more images or biometric information received from the mobile device 112 or watch 134. The data may be, for example, information relating to a user account or instruction to allow access to a separate account information server 120B. The term biometric data may include among other information biometric information concerning facial features and path parameters. Examples of path parameters may include an acceleration and speed of the mobile device, angle of the mobile device during image capture, distance of the mobile device to the user, path direction in relation to the user's face position in relation to the user, or any other type parameter associated with movement of the mobile device or the user face in relation to a camera. Other data may also be included such as GPS data, device identification information, and the like.

[0047] In this embodiment, the server 120 processes requests for identification from the mobile device 112 or user 108. In one configuration, the image captured by the mobile

device 112, using facial detection, comprises one or more images of the user's face 108 during movement of the mobile device relative to the user's face, such as in a side to side or horizontal arc or line, vertical arc or line, forward and backwards from the user's face, or any other direction of motion. In another configuration, the mobile device 112 calculates biometric information from the obtained images, and sends the biometric information to the server 120. In yet another embodiment, the mobile device 112 compares biometric information with stored biometric information on the mobile device 112, and sends a authentication result from the comparison to the server 120.

[0048] The data including either the image(s), biometric information, or both are sent over the network 116 to the server 120. Using image processing and image recognition algorithms, the server 120 processes the person's biometric information, such as facial data, and compares the biometric information with biometric data stored in the database 124 to determine the likelihood of a match. In other embodiments, the image processing and comparison is done on the mobile device 112, and data sent to the server indicates a result of the comparison. In further embodiments, the image processing and comparison is done on the mobile device 112 without accessing the server, for example, to obtain access to the mobile device 112 itself.

[0049] By using facial recognition processing, an accurate identity match may be established. Based on this and optionally one or more other factors, access may be granted or an unauthorized user may be rejected. Facial recognition processing is known in the art (or is an established process) and as a result, it is not described in detail herein.

[0050] Also shown is a second server 120B with associated second database 124B, and third server 120C with associated third database 124C. The second and third database may be provided to contain additional information that is not available on the server 120 and database 124. For example, one of the additional servers may only be accessed based on the authentication of the user 108 performed by the server 120.

[0051] Executing on the mobile device 112 is one or more software applications. This software is defined herein as an identification application (ID App). The ID App may be configured with either or both of facial detection and facial recognition and one or more software modules which monitor the path parameters and/or biometric data. Facial detection as used herein refers to a process which detects a face in an image. Facial recognition as used herein refers to a process that is capable of analyzing a face using an algorithm, mapping its facial features, and converting them to biometric data, such as numeric data. The biometric data can be compared to that derived from one or more different images for similarities or dis-similarities. If a high percentage of similarity is found in the biometric data, the individual shown in the images may be considered to be a match.

[0052] With the ultimate goal of matching a face of a user to an identity or image stored in a database 124, to authenticate the user, the ID App may first process the image captured by the camera 114, 134 to identify and locate the face that is in the image. As shown in Figure 1, there may be the face 108. The authentication may be used for logging into an online account or for numerous other access control functions.

[0053] The portion of the photo that contains the detected face may then be cropped, cut, and stored for processing by one or more facial recognition algorithms. By first detecting the face in the image and cropping only that portion of the face, the facial recognition algorithm need not process the entire image. Further, in embodiments where the facial recognition processing occurs remotely from the mobile device 112, such as at a server 120, much less image data is required to be sent over the network to the remote location. It is contemplated that the entire image, a cropped face, or only biometric data may be sent to the remote server 120 for processing.

[0054] Facial detection software is capable of detecting a face from a variety of angles. However, facial recognition algorithms are most accurate in straight on images in well-lit situations. In one embodiment, the highest quality face image for facial recognition that is captured is processed first, then images of the face that are lower quality or at different angles other than straight toward the face are then processed. The processing may occur on the mobile device or at a remote server which has access to large databases of image data or facial identification data.

[0055] The facial detection is preferred to occur on the mobile device and is performed by the mobile device software, such as the ID App. This reduces the number or size of images (data) that are sent to the server for processing where faces are not found and minimizes the overall amount of data that must be sent over the network. This reduces bandwidth needs and network speed requirements are reduced.

[0056] In another preferred embodiment, the facial detection, facial recognition, and biometric comparison all occur on the mobile device. However, it is contemplated that the facial recognition processing may occur on the mobile device, the remote server, or both.

[0057] Figure 2 illustrates an example embodiment of a mobile device. This is but one possible mobile device configuration and as such it is contemplated that one of ordinary skill in the art may differently configure the mobile device. The mobile device 200 may comprise any type of mobile communication device capable of performing as described below. The mobile device may comprise a PDA, cellular telephone, smart phone, tablet PC, wireless electronic pad, an IoT device, a "wearable" electronic device or any other computing device.

[0058] In this example embodiment, the mobile device 200 is configured with an outer housing 204 configured to protect and contain the components described below. Within the housing 204 is a processor 208 and a first and second bus 212A, 212B (collectively 212). The processor 208 communicates over the buses 212 with the other components of the mobile device 200. The processor 208 may comprise any type processor or controller capable of performing as described herein. The processor 208 may comprise a general purpose processor, ASIC, ARM, DSP, controller, or any other type processing device. The processor 208 and other elements of the mobile device 200 receive power from a battery 220 or other power source. An electrical interface 224 provides one or more electrical ports to electrically interface with the mobile device, such as with a second electronic

device, computer, a medical device, or a power supply/charging device. The interface 224 may comprise any type electrical interface or connector format.

[0059] One or more memories 210 are part of the mobile device 200 for storage of machine readable code for execution on the processor 208 and for storage of data, such as image data, audio data, user data, medical data, location data, accelerometer data, or any other type of data. The memory 210 may comprise RAM, ROM, flash memory, optical memory, or micro-drive memory. The machine readable code as described herein is non-transitory.

[0060] As part of this embodiment, the processor 208 connects to a user interface 216. The user interface 216 may comprise any system or device configured to accept user input to control the mobile device. The user interface 216 may comprise one or more of the following: keyboard, roller ball, buttons, wheels, pointer key, touch pad, and touch screen. A touch screen controller 230 is also provided which interfaces through the bus 212 and connects to a display 228.

[0061] The display comprises any type display screen configured to display visual information to the user. The screen may comprise a LED, LCD, thin film transistor screen, OEL CSTN (color super twisted nematic), TFT (thin film transistor), TFD (thin film diode), OLED (organic light-emitting diode), AMOLED display (active-matrix organic light-emitting diode), capacitive touch screen, resistive touch screen or any combination of these technologies. The display 228 receives signals from the processor 208 and these signals are translated by the display into text and images as is understood in the art. The

display 228 may further comprise a display processor (not shown) or controller that interfaces with the processor 208. The touch screen controller 230 may comprise a module configured to receive signals from a touch screen which is overlaid on the display 228.

[0062] Also part of this exemplary mobile device is a speaker 234 and microphone 238. The speaker 234 and microphone 238 may be controlled by the processor 208. The microphone 238 is configured to receive and convert audio signals to electrical signals based on processor 208 control. Likewise, the processor 208 may activate the speaker 234 to generate audio signals. These devices operate as is understood in the art and as such are not described in detail herein.

[0063] Also connected to one or more of the buses 212 is a first wireless transceiver 240 and a second wireless transceiver 244, each of which connect to respective antennas 248, 252. The first and second transceiver 240, 244 are configured to receive incoming signals from a remote transmitter and perform analog front end processing on the signals to generate analog baseband signals. The incoming signal maybe further processed by conversion to a digital format, such as by an analog to digital converter, for subsequent processing by the processor 208. Likewise, the first and second transceiver 240, 244 are configured to receive outgoing signals from the processor 208, or another component of the mobile device 208, and up convert these signal from baseband to RF frequency for transmission over the respective antenna 248, 252. Although shown with a first wireless transceiver 240 and a second wireless transceiver 244, it is contemplated that the mobile device 200 may have only one such system or two or more transceivers. For example,

some devices are tri-band or quad-band capable, or have Bluetooth®, NFC, or other communication capability.

[0064] It is contemplated that the mobile device, and hence the first wireless transceiver 240 and a second wireless transceiver 244 may be configured to operate according to any presently existing or future developed wireless standard including, but not limited to, Bluetooth, WI-FI such as IEEE 802.11 a,b,g,n, wireless LAN, WMAN, broadband fixed access, WiMAX, any cellular technology including CDMA, GSM, EDGE, 3G, 4G, 5G, TDMA, AMPS, FRS, GMRS, citizen band radio, VHF, AM, FM, and wireless USB.

[0065] Also part of the mobile device is one or more systems connected to the second bus 212B which also interface with the processor 208. These devices include a global positioning system (GPS) module 260 with associated antenna 262. The GPS module 260 is capable of receiving and processing signals from satellites or other transponders to generate location data regarding the location, direction of travel, and speed of the GPS module 260. GPS is generally understood in the art and hence not described in detail herein. A gyroscope 264 connects to the bus 212B to generate and provide orientation data regarding the orientation of the mobile device 204. A magnetometer 268 is provided to provide directional information to the mobile device 204. An accelerometer 272 connects to the bus 212B to provide information or data regarding shocks or forces experienced by the mobile device. In one configuration, the accelerometer 272 and gyroscope 264 generate and provide data to the processor 208 to indicate a movement path and orientation of the mobile device.

[0066] One or more cameras (still, video, or both) 276 are provided to capture image data for storage in the memory 210 and/or for possible transmission over a wireless or wired link or for viewing at a later time. The one or more cameras 276 may be configured to detect an image using visible light and/or near-infrared light. The cameras 276 may also be configured to utilize image intensification, active illumination, or thermal vision to obtain images in dark environments. The processor 208 may process image data to perform image recognition, such as in the case of, facial detection, item detection, facial recognition, item recognition, or bar / box code reading.

[0067] A flasher and/or flashlight 280, such as an LED light, are provided and are processor controllable. The flasher or flashlight 280 may serve as a strobe or traditional flashlight. The flasher or flashlight 280 may also be configured to emit near-infrared light. A power management module 284 interfaces with or monitors the battery 220 to manage power consumption, control battery charging, and provide supply voltages to the various devices which may require different power requirements.

[0068] Figure 3 illustrates exemplary software modules that are part of the mobile device and server. Other software modules may be provided to provide the functionality described below. It is provided that for the functionality described herein there is matching software (non-transitory machine readable code, machine executable instructions or code) configured to execute the functionality. The software would be stored on a memory and executable by a processor.

[0069] In this example confirmation, the mobile device 304 includes a receive module 320 and a transmit module 322. These software modules are configured to receive and transmit data to remote device, such as cameras, glasses, servers, cellular towers, or WIFI system, such as router or access points.

[0070] Also part of the mobile device 304 is a location detection module 324 configured to determine the location of the mobile device, such as with triangulation or GPS. An account setting module 326 is provided to establish, store, and allow a user to adjust account settings. A log in module 328 is also provided to allow a user to log in, such as with password protection, to the mobile device 304. A facial detection module 308 is provided to execute facial detection algorithms while a facial recognition module 321 includes software code that recognizes the face or facial features of a user, such as to create numeric values which represent one or more facial features (facial biometric information) that are unique to the user.

[0071] An information display module 314 controls the display of information to the user of the mobile device. The display may occur on the screen of the mobile device or watch. A user input/output module 316 is configured to accept data from and display data to the user. A local interface 318 is configured to interface with other local devices, such as using Bluetooth® or other shorter range communication, or wired links using connectors to connected cameras, batteries, data storage elements. All of the software (with associated hardware) shown in the mobile device 304 operate to provide the functionality described herein.

[0072] Also shown in Figure 3 is the server software module 350. These modules are located remotely from the mobile device, but can be located on any server or remote processing element. As is understood in the art, networks and network data use a distributed processing approach with multiple servers and databases operating together to provide a unified server. As a result, it is contemplated that the module shown in the server block 350 may not all be located at the same server or at the same physical location.

[0073] As shown in Figure 3, the server 350 includes a receive module 352 and a transmit module 354. These software modules are configured to receive and transmit data to remote devices, such as cameras, watches, glasses, servers, cellular towers, or WIFI systems, such as router or access points.

[0074] An information display module 356 controls a display of information at the server 350. A user input/output module 358 controls a user interface in connection with the local interface module 360. Also located on the server side of the system is a facial recognition module 366 that is configured to process the image data from the mobile device. The facial recognition module 366 may process the image data to generate facial data (biometric information) and perform a compare function in relation to other facial data to determine a facial match as part of an identify determination.

[0075] A database interface 368 enables communication with one or more databases that contain information used by the server modules. A location detection module 370 may utilize the location data from the mobile device 304 for processing and to increase

accuracy. Likewise an account settings module 372 controls user accounts and may interface with the account settings module 326 of the mobile device 304. A secondary server interface 374 is provided to interface and communicate with one or more other servers.

[0076] One or more databases or database interfaces are provided to facilitate communication with and searching of databases. In this example embodiment the system includes an image database that contains images or image data for one or more people. This database interface 362 may be used to access image data users as part of the identity match process. Also part of this embodiment is a personal data database interface 376 and privacy settings data module 364. These two modules 376, 364 operate to establish privacy setting for individuals and to access a database that may contain privacy settings.

Authentication System

[0077] An authentication system with path parameters that is operable in the above described environment and system will now be described in connection with Figure 4. Figure 4 shows a method for performing facial recognition authentication with path parameters according to one embodiment of the invention. As will be described in more detail below, the system utilizes the features of the mobile device 112 and server 120 defined above to generate a secure and convenient login system as one example of an authentication system. This reduces the burden of the user having to type in complex passwords onto a small screen of a mobile device, prevents fraud through means such as

key logging or screen shot captures, and increases security by combining several path parameters and/or device parameters which must be met before user is authenticated.

[0078] In step 410, the system enrolls a user in the facial recognition authentication system. In one embodiment, an authentication server, such as the server 120 (Figure 1), may be configured to authenticate a user to allow access to a user's account, such as a bank or other account, via the mobile device 112. The authentication server 120 may be included as a part of a server of the institution or entity providing user accounts (hereinafter "account server"), or the authentication server may be provided separately. For example, in the environment shown in Figure 1, Servers 120B and 120C may represent account servers. In other embodiments, the account server and the authentication server are one in the same. In one embodiment, the authentication server 120 may provide an authentication application to the user for installation on the mobile device 112.

[0079] An enrollment process according to one embodiment will be described with reference to Figure 5. In this embodiment, a user via a mobile device 112 establishes a connection between the mobile device 112 and the account server 120B in step 510. As just one example, the user may establish a connection with a server of a financial institution such as a bank, or this connection may occur later in the process after authentication. The user then provides typical login information to authenticate the user, such as a user name and password for a financial account in step 512. In step 514, the user may next receive a prompt at the mobile device 112 to enroll in the facial recognition authentication system.

The user then, via the user interface, indicates that he or she would like to set up the authentication system in response to the prompt.

[0080] Next, in step 516, the mobile device 112 may send device information to the authentication server 120. The device information may include among other information a device identifier that uniquely identifies the mobile device of the user. Such information may include device manufacturer, model number, serial number, and mobile network information. In step 518, when the authentication server 120 is incorporated with the account server 120B, the authentication server 120 associates and stores the device information with the user's account information. When the authentication server 120 is separate from the account server 120B, the account server 120B may generate a unique identifier related to the account information and send the unique identifier to the authentication server 120. The authentication server 120 may associate the device information and the unique identifier with each other and may store the information in a database 124.

[0081] The user is next prompted to provide a plurality of images of his or her face using a camera 114 on the mobile device 112 (hereinafter, "enrollment images") in step 510. The enrollment images of the user's face are taken as the user holds the mobile device and moves the mobile device to different positions relative to his or her head and face. Thus, the enrollment images of the user's face are taken from many different angles or positions. Furthermore, the path parameters of the mobile device are monitored and recorded for

future comparison in step 522. Some non-limiting examples of how a user might hold a mobile device and take a plurality of images of her face is shown in FIGS 6A-7B.

[0082] In Figure 6A and 6B, the user holds the mobile device 112 on one side of his or her face, and moves the mobile device 112 in an arc like path horizontally about his or her face until the mobile device 112 is on the other side of her or her face. In FIGS. 7A and 7B, the user holds the mobile device 112 far away from his or her face, and then brings the mobile device 112 forward closer to his or her face. Of course, any number of other paths may be used in addition to those shown in FIGS. 6A-7B. Additionally, the user may move his or her head while the camera is held fixed. The user could also hold the camera steady and move their head in relation to the camera. This method thus can be implemented with a webcam on a laptop or desktop, or on any other device, such as an IoT device where a camera is mounted on a similarly stationary location or object.

[0083] The enrollment images may be obtained as follows. The user holds and orients a mobile device 112 with a camera 114 so that the camera 114 is positioned to image the user's face. For example, the user may use a front facing camera 114 on a mobile device 112 with a display screen and may confirm on the display screen that his or her face is in position to be imaged by the camera 114.

[0084] Once the user has oriented the device, the device may begin obtaining the enrollment images of the user. In one embodiment, the user may press a button on the device 112 such as on a touchscreen or other button on the device to initiate the obtaining

of the enrollment images. The user then moves the mobile device to different positions relative to his or her head as the device images the user's face from a plurality of angles or positions as described above. When the above-mentioned front-facing camera is used, the user may continually confirm that his or her face is being imaged by viewing the imaging on the display screen. The user may again press the button to indicate that the imaging is completed. Alternatively the user may hold the button during imaging, and then release the button to indicate that imaging is complete.

[0085] As described above, the mobile device 112 may include face detection. In this embodiment in step 524, the mobile device may detect the user's face in each of the enrollment images, crop the images to include only the user's face, and send, via a network, the images to the authentication server 120. In step 526, upon receipt of the enrollment images, the authentication server 120 performs facial recognition on the images to determine biometric information ("enrollment biometrics") for the user. The authentication server 120 may then associate the enrollment biometrics with the device information and the unique identifier (or account information) and stores the biometric information in the database 124 in step 528. For added security, in step 530, the mobile device 112 and the authentication server 120 may be configured to delete the enrollment images after the enrollment biometrics of the user are obtained.

[0086] In another embodiment, the mobile device 112 may send the images to the authentication server 120 without performing face detection. The authentication server 120 may then perform the face detection, facial recognition, and biometric information

processing. In another embodiment, the mobile device 112 may be configured to perform the facial detection, facial recognition, and biometric processing, and then send the results or data resulting from the processing to the authentication server 120 to be associated with the unique identifier or user account. This prevents sensitive personal data (images) from leaving the user's device. In yet another embodiment, the mobile device 112 may perform each of the above mentioned steps, and the mobile device 112 may store the enrollment information without sending any of the enrollment biometrics or images to the server.

[0087] In one embodiment, the mobile device's gyroscope, magnetometer, and accelerometer are configured to generate and store data while the user moves the mobile device about his or her head to obtain the enrollment images (path parameters). The mobile device may process this data in step 532 to determine a path or arc in which the mobile device moved while the user imaged his or her face ("enrollment movement"). By using data from the accelerometer, magnetometer, and gyroscope, the system may check when a user is ready to begin scanning himself/herself, as well as determining the scan path. The data is thus used to determine when to start and stop the scan interval. The data may additionally include the time elapsed during scanning. This time may be measured from the user pressing the button to start and stop the imaging, or may be measured from the duration the button is held down while imaging, or during more movement or to complete sweep.

[0088] The enrollment movement of the mobile device 112 (which is data that defined the movement of the mobile device during image capture) may be sent to the authentication

server 120. The authentication server 120 associates and stores the enrollment movement, the enrollment biometrics, the device information, and the unique identifier or account information. Alternatively, the data generated by the gyroscope, magnetometer, and accelerometer may be sent to the server 120, and the server 120 may process the data to determine the enrollment movement.

[0089] Thus, in the above described embodiment, the enrollment information may thus comprise the device information, the enrollment biometrics, and the enrollment movement (based on movement of the mobile device 112).

[0090] Returning to Figure 4, once enrollment is complete, the authentication server 120 may later receive credentials from a user attempting to authenticate with the system as shown in step 420. For example, a user may attempt to log in to a user account. When a user attempts to log in, instead of or in addition to providing typical account credentials such as user name and password, the user may again take a plurality of images or video of his or her face as the mobile device 112 is held in the hand and moved to different positions relative to the head ("authentication images") in the same manner as was done during enrollment (such as shown in FIGS. 6A-7B). In this manner, the user may provide the necessary images (the term images includes video as video is a succession of images) from many different angles and/or positions, and may provide path parameters of the device while obtaining the images ("authentication movement") to both confirm the identity of the user as well as the liveness and realness of that individual to ensure it is not a video, screen shot, or other representation of the person.

[0091] In one embodiment outlined in Figure 8, the user via the mobile device 112 obtains a number of authentication images in step 810 while moving the mobile device 112 to different positions relative to the user's head. Using facial detection in step 812, the mobile device 112 detects the user's face in each of the authentication images, crops the images, and sends the images to the authentication server 120. In another embodiment, the mobile device 112 sends the images to the server 124, and the server 124 performs facial detection. In step 814, the authentication routing 120 may perform facial recognition on the authentication images to obtain biometric information ("authentication biometrics"). In another embodiment, the mobile device 112 performs facial recognition to obtain the authentication biometrics and sends the authentication biometrics to the server 120.

[0092] In step 816, the mobile device 112 sends the device information identifying the device and sends path parameters such as gyroscope, magnetometer, and accelerometer information defining the path of the mobile device taken during imaging, as well as the elapsed time during imaging ("authentication movement") to the server 120. The credentials received by the authentication server 120 for a login in the facial recognition system may thus comprise the device information, the authentication images or the authentication biometrics, and the authentication movement (path parameters).

[0093] Returning to Figure 4, in step 430, the authentication server 120 verifies that the credentials received from the mobile device 112 sufficiently correspond with the information obtained during enrollment. For example, as shown in step 910 in Figure 9, by using algorithms to process the characteristics of the face and light striking the face

between the different images, the authentication server 120 can determine that the face in the authentication images is three-dimensional, i.e. not a representation on a printed picture or video screen. Where the mobile device 120 sends only the authentication biometrics 120 to the server, the server 120 may validate the realness or three-dimensional aspects of the user imaged by comparing the biometric results of the different images.

[0094] In step 920, the authentication server 120 may then compare the login credentials with the information stored from the enrollment process. In step 920, the server 120 compares the identification of the device obtained during the login process to that stored during enrollment. In step 930, the authentication biometrics may be compared with the enrollment biometrics to determine whether they sufficiently correspond with the enrollment biometrics. In step 940, the authentication movement may be compared with the enrollment movement to determine whether it sufficiently corresponds with the enrollment movement.

[0095] In some embodiments, a copy of the enrollment information may be stored on the mobile device 112, and the mobile device 112 may verify that the credentials received on the mobile device 112 sufficiently correspond with the enrollment information. This would allow a user to secure documents, files, or applications on the mobile device 112 itself in addition to securing a user's account hosted on a remote device, such as the authentication server 120, even when a connection to the authentication server 120 may be temporarily unavailable, such as when a user does not have access to the Internet. Further, this would

allow the user to secure access to the mobile device 112 itself. Or enrollment info may be stored on server.

[0096] Accordingly, in step 950, if the authentication server 120 or mobile device 112 determines that the enrollment information sufficiently corresponds with the credentials received, then the server or mobile device may verify that the identification of the user attempting login corresponds the account holder. This avoids the cumbersome process of the user having to manually type in a complex password using the small screen of the mobile device. Many passwords now require capital, non-text letter, lower case, and numbers.

[0097] The level of correspondence required to determine that the enrollment information sufficiently corresponds with the authentication information in the login attempt may be set in advance. For example, the level of correspondence may be a 99.9% match rate between the enrollment biometrics and the authentication biometrics and a 90% match rate between the enrollment movement and the authentication movement. The required level of correspondence may be static or elastic based on the established thresholds.

[0098] For example, the required level of correspondence may be based on GPS information from the mobile device 112. In one embodiment, the authentication server 120 may require a 99.9% match rate as the level of correspondence when the GPS information of the mobile device corresponds with the location of the user's home or other authorized location(s). In contrast, if the GPS information shows the device is in a foreign

country far from the user's home, the authentication server may require a 99.99% match rate as the level of correspondence or may be denied entirely. Hence, the required match between pre-stored authentication data (enrollment information) and presently received authentication data (authentication information) is elastic in that the required percentage match between path parameters or images my change depending on various factors, such as time of day, location, frequency of login attempt, date, or any other factor.

[0099] The required level of correspondence may additionally depend on time. For instance, if a second authentication attempt is made shortly after a first authentication attempt in a location far from the first authentication location based on GPS information from the mobile device 112, the level of correspondence threshold may be set higher. For example, a user can not travel from Seattle to New York in 1 hour. Likewise, login attempts at midnight to three in the morning may be a sign of fraud for some users based on patterns of the users' usage.

[0100] The level of correspondence between the enrollment information and the authentication information may be the result of compounding the various parameters of the enrollment information and the authentication information. For example, when the button hold time in the authentication information is within 5% of the button hold time of the enrollment information, the correspondence of the button hold time may constitute 20% of the overall match. Similarly when the motion path trajectory of the authentication information is within 10% of the enrollment information, the motion path trajectory may constitute 20% of the overall match. Further parameter match rates such as the face size

and facial recognition match in the authentication information as compared to the enrollment information may constitute the remaining 10% and 50% of the overall level of correspondence. In this manner, the total overall level of correspondence may be adjusted (total of all parameters being more than 75%, for example), or the match rate of individual parameters may be adjusted. For example, on a second attempted login, the threshold match rate of one parameter may be increased, or the overall level of correspondence for all parameters may be increased. The threshold match rates may also be adjusted based on the account being authenticated or other different desired levels of security.

[0101] Returning to Figure 4, in step 440, the authentication server 120 may grant or deny access based on the verification in step 430. For example, if the authentication server 120 verifies that the credentials match the enrollment information, then the server 120 may authenticate the user to allow access to the user's account. In the instance where the authentication server 120 is separate from the account server 120B (such as a bank's server), the authentication server 120 may transmit the unique identifier to the account server along with an indication that the identity of the user associated with the unique identifier has been verified. The account server 120B may then authorize the user's mobile device 112 to transmit and receive data from the account server 120B. Of course, all this may occur at only the account server 120B or on the mobile device 112 itself.

[0102] Alternatively, if the credentials provided by the user are not verified, the authentication server may transmit a message to display on the screen of the mobile device 112 indicating that the login attempt failed. The authentication server 120 may then allow

the user to try again to log in via the facial recognition login system, or the authentication server 120 may require the user to enter typical account credentials, such as a user name and password.

[0103] In one embodiment, the server 120 may allow three consecutive failed login attempts before requiring a user name and password. If in one of the attempts, the required level of correspondence is met, then the user may be verified and access may be granted. According to one embodiment, the authentication server 120 may retain the information from each successive authentication attempt and combine the data from the multiple authentication attempts to achieve more accurate facial biometric information of the person attempting to authenticate. In addition, the level of correspondence may be increased at each successive attempt to authenticate. In addition, by averaging the path data (authentication movement) and/or image data (authentication images/biometrics) from several login attempts, the login data (enrollment information) is perfected and improved.

[0104] Accordingly, the above described authentication system allows for authentication to a remote server 120 or on the mobile device 112 itself. This may be accomplished as described above by the mobile device 112 capturing the authentication credentials, and the authentication server 120 processing and analyzing the credentials compared to the enrollment information (cloud processing and analysis); the mobile device 112 capturing the authentication credentials and processing the credentials, and the authentication server 120 analyzing the credentials compared to the enrollment information (mobile device processing, cloud analysis); or the mobile device 112 capturing the authentication

credentials, and processing and analyzing the credentials compared to the enrollment information (mobile device processing and analysis).

Advantages and Features of the Embodiments

[0105] The above described system provides a number of advantages. As one advantage, the facial recognition authentication system provides a secure login. For example, if during a login attempt the camera of the mobile device imaged a digital screen displaying a person rotating their head while the phone was not moving, the accelerometer, magnetometer, and gyroscope data would not detect any motion. Thus, the enrollment movement and the authentication movement would not correspond, and the login attempt would be denied.

[0106] In addition, because a plurality of images are used as enrollment images and authentication images, histograms or other photo manipulation techniques may be used to determine if a digital screen is present in place of a human face in the images. For example, the system may check for light frequency changes in the captured images, or banding in an image which would indicate an electronic display generated the image, backlighting, suspicious changes in lighting, or conduct other analyses on the images by comparing the images to determine that the actual live user is indeed alive, present, and requesting authorization to login.

[0107] As yet another advantage, as explained above, not only must the enrollment biometrics sufficiently correspond to the authentication biometrics, but also the enrollment movement must match the authentication movement, and the device information must

match the enrollment device information. For example, an application may be downloaded to a mobile device that has a digital camera. The application may be a login application, or may be an application from a financial institution or other entity with which the user has an account. The user may then login to the application using typical login credential such as a website user name and password. Further, the user may have a device code from logging in on another device, or may use the camera to scan QR code or other such code to pair the device to their user account.

[0108] The user then holds the mobile device to move the mobile phone to different positions relative to his or her head while keeping his or her face visible to the camera as it is moved. As the mobile device is moved, the camera takes the enrollment images of the face. During imaging, the speed and angle of the current user's mobile device movement is measured using the accelerometer, magnetometer, and gyroscope to generate the enrollment movement. Further continuous imaging and detection of the face throughout the process has been shown to prevent fraud. This is because a fraud attempt cannot be made by rotating images in and out of the front of the camera.

[0109] For example, a user may start the movement from right to left or from left to right as shown in FIGS. 6A and 6B. The movement may also be in a front and back direction as shown in FIGS. 7A and 7B. Any other movement may be utilized such as starting in the center, then going right, and then going back to center. Vertical and diagonal movements may also be used to further compound the complexity of the enrollment movement. When the user then later attempts login, the user must repeat the motion pattern

in the authentication movement so as to match the enrollment movement in addition to the biometric data and device information matching. Thus, the security of the system is greatly enhanced.

[0110] The system therefore provides enhanced security for authenticating a user who has a mobile device. As explained above, the system may use at least any one or more of the following in any number of combinations to securely authenticate the user: physical device verification, mobile network verification, facial recognition including the size of the face in the image, a face detected in every frame during the movement, accelerometer information, gyroscope information, magnetometer information, pixels per square inch, color bits per pixel, type of image, user entered code or pattern, and GPS information.

[0111] As another advantage, the facial recognition login system provides a convenient manner for a user to login to an account with a mobile device. For example, once enrolled, a user does not need to enter a user name and password on the small mobile device each time the user wishes to access the account. Instead, the user simply needs to image himself or herself while mimicking the enrollment movement with the mobile device. This is especially advantageous with smaller mobile devices such as mobile phones, smart watches, and the like.

[0112] The system may be further configured to allow a user to securely log on to multiple devices, or to allow users to securely share devices. In one embodiment, the enrollment information may be stored on an authentication server (or on "the cloud") and thus is not

associated only with the user's original device. This allows the user to use any number of suitable devices to authenticate with the authentication server. In this manner, a user may use a friend's phone (third party device) or other device to access his or her information, such as account information, address book information, email or other messaging, etc. by performing the authentication operation on any device.

[0113] For example, the user may provide an email address, user name code, or similar identifier on the friend's phone such that the authentication server compares the login information with enrollment information for the user's account. This would indicate to the authentication server which authentication profile to use, but does not by itself allow access to the user's data, accounts, or tasks. Upon logging out of a friend's phone, access to the user's information on the friend's phone is terminated. The provides the benefit of allowing a user to securely access account or other authentication accessible information or tasks using any device without having to type the user's password into the third party device, where it could be logged or copied. In a sense, the user is the password.

[0114] Through cloud-based enrollment information, a single user may also securely transfer data between authenticated devices. In one embodiment, a user may own a first device, such as a mobile phone, and is authenticated on the first device via the authentication system. The user may then acquire a new device, such as a new phone, tablet computer, or other device. Using the cloud-based authentication system, the user may authenticate on the new device and transfer data from the first device to the new device. The transfer of data may be completed via the Internet, a local network connection,

a Bluetooth connection, a wired connection, or a near field communication. The authentication process may also be part of a security check to resent or restore a system after the phone is lost or stolen. Thus, the authentication system may be used to activate or authenticate a new device, with the authentication used to verify the user of the new device.

[0115] Similarly, the system may facilitate secure access to a single shared device by multiple people to control content or other features on the device. In many cases, passwords can be viewed, copied, guessed, or otherwise detected, particularly when a device is shared by a number of users. The users may be, for example, family members including parents and children, coworkers, or other relationships, such as students. The authentication system may allow each of the family members to log in based on his or her own unique enrollment information associated with a user account.

[0116] The device may restrict access to certain content or features for one or more of the certain user's accounts, such as children's user accounts, while allowing access to content and features for others, such as the parents' accounts. By using the authentication system for the shared device, the users such as children are unable to utilize a password to try and gain access to the restricted content because the authentication system requires the presence of the parent for authentication, as explained above. Thus device sharing among users with different privileges is further secured and enhanced. Likewise, in a classroom setting, a single device may be securely shared between multiple people for testing, research, and grade reporting.

Adaptations and Modifications

[0117] Numerous modifications may be made to the above system and method without departing from the scope of the invention. For example, the images may be processed by a facial recognition algorithm on the device and may also be converted to biometric data on the device which is then compared to previously created biometric data for an authorized user. Alternatively, the images from a device may be sent through a wired or wireless network where the facial recognition algorithms running on a separate server can process the images, create biometric data and compare that data against previously stored data that assigned to that device.

Multiple Profiles for a Single User

[0118] Further, the photo enrollment process may be done multiple times for a user to create multiple user profiles. For example, the user may enroll with profiles with and without glasses on, with and without other wearable devices, in different lighting conditions, wearing hats, with different hair styles, with or without facial or ear jewelry, or making different and unique faces, such as eyes closed, winking or tongue out to establish another level of uniqueness to each user profile. Such 'faces' made by the user would not be available on the user's Social Media Pages and hence not available for copying, manipulation, and use during a fraud attempt. Each set of enrollment images, enrollment biometrics, or both may be saved along with separate enrollment movement. In one embodiment at least three images are captured as the mobile device completes the path. It is contemplated that any number of images may be captured.

Linking Enrollment Information

[0119] It is also contemplated that the enrollment process may be linked to an email address, phone number, or other identifier. For example, a user may sign up with an email address, complete one or more enrollments as described above, and confirm the enrollments via the same email address. The email address may then further enhance the security of the system. For example, if a user unsuccessfully attempts to login via the authentication system a predetermined number of times, such as three times for example, than the authentication system locks the account and sends an email to the email address informing the user of the unsuccessful login attempts. The email might also include one or more pictures of the person who failed to login and GPS or other data from the login attempt. The user may then confirm whether this was a valid login attempt and reset the system, or the user may report the login attempt as fraudulent. If there is a reported fraudulent login, or if there are too many lockouts, the system may delete the account associated with the email address to protect the user's security. Thus, future fraudulent attempts could not be possible.

Feedback Meters

[0120] To further facilitate imaging, the mobile device may include various feedback meters such as a movement meter or accuracy meter as shown in Figure 10. In one embodiment, the mobile device 1012 may display a movement meter 1024 that indicates the amount of movement the mobile device 1012 makes as the user moves the mobile

device 1012 to different positions relative to his/her head. For example, the movement meter 1024 may be represented as a line that slides from one side of the screen. In this manner, the enrollment process may require a certain threshold of device movement in order to register a user with the multi-dimensional authentication system. For example, the system could require that the mobile device 1012 is moved in an arc or straight line and rotate at least 45 degrees in order to create the enrollment information. In another example, the system could require an acceleration experienced by the device exceeding a threshold amount. The movement meter may also aid the user in learning how to image himself/herself using the authentication system.

[0121] The mobile device 1012 may also display an accuracy meter 1026 or any other visual representation of authenticated frames to aid the user in authenticating himself/herself using the authentication system and learning to improve authentication. The accuracy meter 1026 may show a user a match rate (graphical, alpha, or numerical) of a predetermined number of images obtained during the authentication process. The accuracy meter can be represented on the display in a variety of ways including numeric percentages, color representation, graphical, and the like. A combination of representations may also be utilized.

[0122] For example, as shown in Figure 10, match rates for a predetermined number of images taken during authentication are represented on the accuracy meter. In the embodiment shown in Figure 10, each of the images may be represented by a column in a graph, and the accuracy can be shown for each image in each column. For example, the

column with a longer bar represent higher accuracy, and a column with a lower bar represents lower accuracy. In addition to match rates for images, the match rates for the path parameter may also be displayed. Over time the user can improve.

[0123] In another embodiment, each of the images may be represented on a table as a color that corresponds to the match rate. The color dark green may represent a very high match rate, light green may represent a good match rate, yellow may represent a satisfactory match rate, red may represent a mediocre match rate, and grey may represent a poor match rate. Other colors schemes may also be used.

[0124] The height of the bars or the colors used may correspond to predetermined match rates. For example, a full bar or dark green may be a match rate greater than 99.9%, a three-quarter bar or light green may be a match rate between 90% and 99.9%, a half bar or yellow may be a match rate of 50-90%, red may be a match rate of 20%-50%, and a single line to a quarter bar or grey may be a match rate of 0-20%. A pie chart, line graph, or any other type of representation could also be used or any other numerical or graphical display. An overall score may be presented or a score per image.

[0125] The accuracy meter may also include a message 1028 indicating an overall match score. For example, the accuracy meter may indicate an average overall match score or the number of images which achieved a 99.9% match rate, and display the message to a user. With the movement meter 1024 and the accuracy meter 1026 as described above, the user

may quickly learn to use the authentication system due to the feedback presented by the meters 1024, 1026.

Gamification and Rewards

[0126] The movement and accuracy meters 1024, 1026 may also be configured to incorporates game features, aspects, or techniques into the authentication system to encourage a user to try and get the best match possible (such as a high number score or a high percentage of frames), increasing the user's skill in utilizing the authentication system. This also builds user adoption rates for the technology.

[0127] For example, the user may compete with themselves to mimic or improve past authentication scores to encourage or train the user to achieve a high score. Further modifications of the authentication meter may also be incorporated such as the ability to share accuracy match results with others to demonstrate one's skill in using the system or to compete against others. In other instances the user may receive a reward, such as a gift or coupon, for high accuracy scores. While this may slightly increase costs, the reduction in fraud loss would far outweigh the additional cost.

[0128] Further game techniques may be incorporated into the authentication system to encourage users to take actions which will prevent unauthorized or fraudulent authentication. In one embodiment, the authentication system may award users that engage in fraud preventing activities. One such activity is utilizing the facial recognition

authentication system described herein. For example, based on the above described accuracy meter, the system may reward a user that successfully authenticates with the system above a certain match rate. The system may award reward points, cash, or other prizes based on the successful authentication or on a predetermined number of successful authentications. Where reward points are utilized, the points may be cashed in for predetermined prizes.

[0129] Other game features may involve award levels for users who gain a predetermined amount of experience using the authentication feature. For example, different reward levels may be based on users successfully authenticating 100 times, 500 times, 1000 times, etc. Because each instance of fraud loss can be significant and can damage the goodwill of the business or organization, the benefits to fraud prevention are significant.

[0130] In one embodiment, the user may be notified that he or she has achieved various competency levels, such as a "silver level" upon achieving 100 successful authentications, a "gold level" for achieving 500 successful authentications, or a "platinum level" for achieving 1000 successful authentications. A number of points awarded for each authentication above a given match rate may increase based on the user's experience level. Of course, the names of the levels and the number of authentications for each level as described above are only exemplary and may vary as desired.

[0131] In one embodiment, an authentication only counts toward reward levels when business is transacted at the web site while in other embodiments, repeated attempts may

be made, all of which count toward rewards. Another feature may incorporate a leaderboard where a user may be notified of a user ranking comparing his or her proficiency or willingness in using the authentication system as compared with other users.

[0132] Successful use of the authentication system benefits companies and organizations that utilize the system by reducing costs for fraudulent activities and the costs of preventing fraudulent activities. Those cost savings may be utilized to fund the above described game features of the authentication system.

[0133] Further activities that correspond to the authentication system and contribute to the reduction of fraud may also be incorporated to allow a user to earn points or receive prizes. Such activities may include a user creating a sufficiently long and strong password that uses a certain number and combination of characters. This encourages and rewards users to set passwords that are not easily compromised. Other examples may include rewarding users to take time to perform verification steps in addition to an initial authentication such as a mobile phone or email verification of the authentication, answering one or more personal questions, or other secondary verifications as currently known or later developed. This rewards users for taking on added time and inconvenience to lower the risk of fraud to a company or organization.

[0134] As another example, if the authentication service is used to login to websites or apps that provide affiliate programs, then the reward or gift can be subsidized from the affiliate commissions on purchases made on those sites. For example, if a commerce

(product or service) web site utilizes the method and apparatus disclosed herein to avoid fraud, and thus increase profits, then a percentage of each purchase made by a user using the authentication service will be provided to the authentication service. By reducing fraud, consumer purchases are more likely and additional users will be willing to enter financial and personal information. An affiliate link, code, or referral source or identifier may be used to credit the authentication system with directing the consumer to the commerce (product or service) web site.

Multiple Account Login

[0135] It is also contemplated that the authentication system may be configured to allow a user to access a number of different web sites as a result of a single authentication. Because the authentication process and result is unique to the user, the user may first designate which participating web sites the user elects to log into and then after selecting which one or more web sites to log into, the user performs the authentication described herein. If the secure authentication is successful, then the user is logged into the selected web sites. In this way, the authentication process is a universal access control for multiple different web sites and prevents the user from having to remember multiple different user names and passwords while also reducing fraud and password overhead for each user.

Automatic Start/Stop of Imaging

[0136] It is also contemplated that the system may be configured to have the video camera running on the phone. The mobile device would grab frames and path parameter data when the phone moves (using the camera, gyroscope, magnetometer, and accelerometer) but only process into biometric data on the device or send the frames up to the server if they have a face in them. In this embodiment, the application executing on the mobile device could trigger the software application to start saving frames once the phone is moving and then if the phone continues to move in the correct path (a semi-circle, for example) and the system detects a face in the frame the mobile device would start to send images, a portion of the image, or biometric data to the server for processing. When the system senses motion it may trigger the capture of images at certain intervals. The application may then process the frames to determine if the images contain a face. If the images do include a face then the application crops it out and then verifies if the motion path of the mobile device is similar to the one use used during enrollment. If the motion path is sufficiently similar, then the application can send the frames one at a time to the server to be scanned or processed as described above.

Banding and Edge Detection

[0137] When a fraudulent attempt is made using a display screen, such as an LED, LCD, or other screen, the system may detect the fraudulent login attempt based on expected attributes of the screen. In one embodiment, the authentication system will run checks for banding produced by digital screens. When banding is detected, the system may recognize a fraudulent attempt at a login. In another embodiment, the system will run checks for

edge detection of digital screens. As the mobile device is moved to obtain the authentication movement during a login attempt, the system checks the captured images to for edges of a screen to recognize a fraudulent login attempt. The system may also check for other image artifacts resulting from a screen such as glare detection. Any now know or later developed algorithms for banding and screen edge detection may be utilized. Upon detection of fraud will prevent authentication and access to the website or prevent the transaction or account access.

Other Attributes Estimation

[0138] The authentication system may further conduct an analysis on the enrollment images to estimate at least one of a gender, an approximate age, and an ethnicity. In an alternative embodiment, the user may manually enter one or more of their gender, an approximate age, and an ethnicity, or this information may be taken or obtained from existing records which are known to be accurate. The authentication system may then further store a user's estimated gender, age, and ethnicity as enrollment credentials or user data. Thus when the user later attempts to authenticate with the system, the system will compare derived gender, age, and ethnicity obtained from authentication images (using biometric analysis to determine such data or estimates thereof based on processing) with the stored gender, age, and ethnicity to determine whether or not to authenticate the user. For example, if the derived data for gender, age and ethnicity matches the stored enrollment credentials, then the authentication is successful or this aspect of the authentication is successful.

[0139] The authentication system may make the gender, age, and ethnicity estimations based on a single image during the authentication process or based on multiple images. For example, the authentication system may use an image from the plurality of images that has an optimal viewing angle of the user's face for the analysis. In other embodiments, a different image may be used for each analysis of age, gender, and ethnicity when different images reveal the best data for the analysis. The authentication may also estimate the gender, age, and ethnicity in a plurality of the images and average the results to obtain overall scores for a gender, age, and ethnicity.

[0140] As an alternative to obtaining the gender, age, and ethnicity as enrollment information, the estimated gender, age, and ethnicity estimations as authentication credentials may be set over a course of repeated use of the authentication system. For example, if in previous successful authentications using biometrics and movement information, the authentication system always estimates a user's age being between 40 and 50, then the authentication may set credentials for that user requiring later login information to include images of a face estimated to be between 40 and 50. Alternatively, gender, age, and ethnicity estimations may be implemented as one of many factors contributing to an overall authentication score to determine whether or not to authenticate a user.

[0141] For example if the authentication process has a gender estimation of + or - 0.2 of 1.9 male rating, then if the actual results do not fall within that range the system may deny access for the user. Likewise, if the user's age range always falls between 40-50 years of

age during prior authentication attempts or enrollment, and an authentication attempt falls outside that range, the system may deny access or use the result as a compounding factor to deny access.

[0142] In a further embodiment, when a bracelet or watch capable of obtaining an EKG signature is used, a certain EKG signature may be required at login. The EKG signature could also be paired with the facial recognition rotation to provide multiple stage sign-on for critical security and identification applications. Further, the credentials could also include GPS information where login is only allowed within certain geographic locations as defined during enrollment. In one configuration the GPS coordinates of the mobile device are recorded and logged for a login attempt or actual login. This is additional information regarding the location of the user. For example, if the GPS coordinates are in a foreign country known for fraud, then the attempt was likely fraudulent, but if the GPS coordinate indicate the attempt or login was made in the user's house, then fraud is less likely. In addition some applications may only allow a user to login when at specified location such as a secure government facility or at a hospital.

[0143] The enrollment information may further include distance information. Because the motion arc (speed, angle, duration…) is unique to each user, face detection software on the device can process the images and determine if the device is too close or too far from the subject. Or in other words, the enrollment information may take into account the size of the face in the images. Thus the potential enrollment information may also vary based on the length of a user's arm, head, and face size, and on the optics of the camera in the user's

particular mobile device. The user may also be positioned at a fixed computer or camera, such as laptop, desktop, or atm. The user may then move the face either forwards and back, side to side, or up and down (or a combination) to create the images. Hence, this method of operation is not limited to a mobile device. In one embodiment, the camera is located in an automobile, such as in a mirror, and the person moves their head or face to authenticate.

Gradual Authentication Access

[0144] In one embodiment, the system is set to limit what the user can do when first enrolled and authenticated. Then, after further authentications or after a predetermined time period and number of authentications, additional capabilities may be granted. For example, during the first 20 authentications during the first 3 months, a maximum transaction of $100 may be allowed. This builds of database of known authentication data in connection with non-objected to transactions by the user. Then, during the next 20 authentications a transaction limit of $3000 may be established. This limits the total loss in the event of fraud when the authentication data is limited and the user is new to the system, for example if an unauthorized user is able to fraudulently enroll in the authentication system.

Video Display for Imaging

[0145] When the user images himself/herself using a front-facing camera, the user may confirm that his/her face is being imaged by viewing the image on the display, as described above. The image shown on the display may be configured so as to be smaller in area than the entire display, and may be positioned in an upper portion of the display towards the top of the device. When the user's image is shown only in the top portion of the user's display screen, the user's eyes tend to look more closely at the front camera. When the user's eyes are tracking up, the accuracy of the facial recognition may be improved. Further, tracking the movement of the eyes from frame to frame may allow the system to validate that the images are of a live person, and are not from a photograph or video recording of the person.

[0146] The image shown on the display may also be positioned to correspond with a camera location on the user's device, as shown in FIGS 11A-11C. Mobile devices that are available today may include front-facing cameras disposed at a number of different positions. For example, one mobile device 1112a, 1112,b may have a front-facing camera 1114a, 1114b that is disposed above the display and off center towards one side or the other, as shown in FIGS 11A and 11B. Accordingly, the feedback image 1116a, 1116b of the user shown on the display may be positioned so as to correspond with the location of the camera 1114a, 1114b as shown. In FIG 11A, where a camera 1114a is above the display and is off-center at a position left of the center, then the image 1116a may be shown in an upper left corner of the display. In FIG 11B, where a camera 1114b is above the display and is off-center at a position right of the center, then the image 1116b may be shown in

an upper right corner of the display. As shown in Figure 11C, a mobile device 1112c may have a camera 1114c that is disposed centered directly above the display. There, the image 1116c may be displayed centered in an upper portion of the display. In this manner, a user's eyes are directed close to and/or track as close to the camera as possible, aiding eye tracking and movement verification. The user is also able to better see the feedback image, and other feedback or information on the screen, as they move the mobile device.

[0147] The image viewed on the display by the user may further be modified such that the edge pixels on the sides display are stretched horizontally as shown in Figure 12. That is, a predetermined area 1206, 1208 on both the right and the left sides are warped to stretch towards right and left edges, respectively, of the screen. This allows a larger vertical portion of the displayed image to be shown on the display. Simultaneously, this trains a user to use the system correctly by keeping his or her face in the center of the screen, as his or her face would become warped on the screen if it becomes off center and part of the face enters the one of the warped areas.

Authentication in Low-light Environments

[0148] To facilitate imaging, the screen on the mobile device may additionally be displayed with a white background, and the brightness of the screen may be increased to light up the user's face in dark environment. For example, a portion of the display could provide video feedback for the user to ensure he or she is imaging himself or herself, while the remaining portion of the display is configured to display a bright white color. Referring

back to the example shown in Figure 11C, this may be done by showing the video feedback 1116c on a center of the display, with the surrounding areas being displayed as bright white bars around the video feedback 1116c. In very dark situation, an LED flash on the back side of the mobile device and the back facing camera may be used. Alternatively, the camera may be configured to create an image using infrared light or other night vision techniques.

[0149] When infrared imaging is used as thermal imaging, further security enhancements are possible. Particularly, the thermal imaging may be analyzed to indicate whether or not the obtained images are from an actual user or are fraudulent images from a screen or other device. When a person is in front of an infrared thermal imaging camera, the heat radiation detected should be fairly oval shaped designating the person's head. In contrast, the heat radiating from a screen is typically rectangular. Further, the heat patterns detected in the actual person's face as well as the movement of the heat patterns in the images can be compared with expected heat patterns of a human face so as to distinguish the images from fraudulent authorization attempts using a screen.

Detecting Output from the Mobile Device

[0150] The display or other light source on the mobile device may further be utilized to provide additional security measures. During the authentication process described above, light from the display or other light source is projected onto the user's face and eyes. This projected light may then be detected by the camera of the mobile device during imaging.

For example, the color tone detected on the skin, or a reflection of the light off of the cornea of a user's eye may be imaged by the camera on the mobile phone. Because of this, random light patterns, colors, and designs may be utilized to offer further security and ensure there is a live person attempting authentication and not merely an image or video of a person being imaged by a fraudster.

[0151] As one example, when a user begins authentication, the authentication server may generate and send instructions to the user's device to display a random sequence of colors at random intervals. The authentication server stores the randomly generated sequence for later comparison with the authentication information received from the mobile device. During authentication imaging, the colors displayed by the device are projected onto the user's face, and are reflected off of the user's eyes (the cornea of the eyes) or any other surface that receives and reflects the light from the screen. The camera on the user's mobile device detects the colors that are reflected off of the user's skin or eyes (or other surface) and generates color data indicating the colors detected based on the screen projection. This data may be returned to the authentication server to determine if the color sequence or pattern sent to the mobile device matches that known sequence or pattern projected by the screen of the user device. Based on this comparison at the authentication server the authentication is a success or denied. The comparison with the random sequence of colors in the instructions may alternatively occur exclusively at the user device to determine that a live user is being authenticated.

[0152] As another example, when a user begins authentication, the authentication server may send instructions the user's device to display a randomly generated pattern which is then stored on the authentication server. This pattern may include graphics, text, lines or bars, flashing light patters, colors, a QR code, or the like. The randomly generated pattern is displayed during authentication imaging, and the pattern is reflected off of the user's eyes (cornea). The camera of the user's device detects the reflected pattern off of the eye of the user and processes the reflected, mirrored image of the displayed pattern. The processed pattern (such as being converted to a numeric value) is transmitted to the authentication server and compared to the pattern that was randomly generated and stored on the authentication server to verify if the pattern displayed by the screen, and imaged after reflection off the user's face establishes a pattern match.

[0153] If a match occurs, this establishes or increases the likelihood that a live person is being imaged by the device. If the pattern is not a match, or does not meet a match threshold level, then the authentication process may fail (access denied) or the account access or transaction amount may be limited. It is noted that this example could also be incorporated on desktop computer with a webcam that does not incorporate the enrollment movement and authentication movement described above. Further, this example may not only be incorporated with facial recognition, but could also serve as an added layer of security for iris recognition or any other type of eye blood vessel recognition, or any facial feature that is unique to a user.

[0154] When the above example is implemented on a desktop computer, eye tracking may also be utilized to further demonstrate the presence of a live user. For example, the screen could show a ball or other random object or symbol moving in a random pattern that the user watches with his or her eyes. The camera can detect this real time movement to verify the user is live, and not a picture or display, and verify that the eye or head movements correspond to and match the expected movement of the object or words on the screen, which are known by the authentication system. Eye tracking can also be done by establishing an anchor point, such as via a mouse click at a location on the screen (assuming that the user is looking at the location where the mouse click takes place), and then estimating where the user is looking at the screen relative to the anchor position.

[0155] The use of a moving object on the screen may also be beneficial during enrollment on either a mobile or stationary device. For example, while capturing the enrollment images, the device may display a moving digital object (such as a circle or words(s)) that moves around the screen so that the user is encouraged to follow it with his or her head and eyes. This movement may be involuntary from the user, or the device may be configured to instruct the user to follow the object. This results in movement of the head and/or eyes creating small changes in the orientation of the user's head and face with the device camera, providing more complete enrollment information. With more complete enrollment information, the system may better ensure that the user will later be authenticated at a high rate even at slightly different angles during future authentication attempts.

Intuitive User Training and Enhanced Security by "Zooming"

[0156] In one embodiment, the system is configured to aid the user to easily learn to authenticate with the system. As shown in Figure 13A, once enrollment or authentication is begun as described previously, the system causes the user's mobile device 1310 to display a small oval 1320 on the screen 1315 while the mobile device 1310 is imaging the user. Instructions 1325 displayed on the screen 1315 instruct the user to hold the mobile device 1310 so that his or her face or head appears within in the oval 1320. Because the oval 1320 is small, the user is required to hold the mobile device 1310 away from his or her body, such as by straightening his or her arm while holding the mobile device 1310. The maximum arm length and face size is unique to the user. In other embodiment, the arm may not be fully straightened such as to accommodate operation when space is not available, such as in a car or in a crowded location. It is noted that while the small oval 1320 is shown centered in the display, it may be positioned anywhere on the screen 1315.

[0157] Next, as shown in Figure 13B, the system causes the user's mobile device 1310 to display a larger oval 1330 on the display 1315. The display 1315 may also show corresponding instructions 1335 directing the user to "zoom in" on his or her face in order to fill the oval 1330 with his or her face. The user does this by bringing the mobile device 1310 closer to his or her face in a generally straight line to the user's face (such as shown in FIGS. 7A and 7B) until the user's face fills the oval 1330 or exceeds the oval. In other embodiments, the large oval 1330 may simply be a prompt for the user to bring the mobile device 1310 closer to the user's face.

[0158] Thus, the system provides and teaches the user a simple method to provide enrollment and authentication images along with enrollment and authentication movement as explained above. The system may also teach varying enrollment and authentication movement by varying the location of the small oval 1320 on the screen 1315, and by changing the order and the size of the ovals displayed. For example the user may zoom in ½ way, then out, then in all the way, by moving the mobile device. The system may be configured to monitor that the camera's zoom function (when equipped) is not in use, which typically requires the user to touch the screen.

[0159] In one embodiment, the enrollment movement may be omitted, and the authentication movement may be compared to expected movement based on the prompts on the screen. For example, the device or authentication server generates a series of differently sized ovals within which the user must place his or her face by moving the mobile device held in the user's hand. In this manner, the authentication movement may be different during each login depending on the order, size, and placement of the ovals shown on the screen.

[0160] The system may also incorporate other security features when the "zoom in" movement is used as shown in Figures. 13A and 13B. Typical cameras on a mobile device or any other device include a curved lens. This results in a "fish-eye" effect in the resulting images taken by the camera. In some instances, this curvature may not be visible to the human eye, or may only be noticeable at certain focal lengths. The curvature or fish eye effect can vary with focal length or distance between the user and the lens. The degree of

the fish-eye effect is dependent on the type of optics used in the camera's lens and other factors.

[0161] The fish-eye effect becomes more pronounced on an image of a person's face when the person images his or her face close to the lens. The effect results in the relative dimensions of the person's face appearing different than when the imaging is done with the person's face farther away from the lens. For example, a person's nose may appear as much as 30% wider and 15% taller relative to a person's face when the image is taken at a close proximity as compared to when the image is taken at a distance. The differences in the relative dimensions are caused by the relatively larger differences in focal length of the various facial features when the person is imaged close to the lens as compared to the relatively equal distances in focal length when the person is imaged at a distance farther from the lens.

[0162] Such differences have been found to be significant in many facial recognition algorithms. That is, a facial recognition algorithm may not recognize a live person imaged at a close proximity and a far proximity as the same person. In contrast, if a two dimensional photograph of a person is imaged by the camera at both a close proximity and a farther proximity, the relative focal lengths between the lens and the two-dimensional image do not change so significantly. Thus, a facial recognition algorithm would recognize the two-dimensional photograph as the same person when imaged at both a close proximity and a distance farther from the lens.

[0163] This effect may be used to increase the security of the authentication system. For example, during enrollment, enrollment images may be provided by the user at both the close and far proximity from the lens, in addition to other positions through the movement. Later, during authentication, authentication images may be obtained at both the close and far distances from the lens to determine if they match with the enrollment information obtained from the enrollment images. Further, because the fish-eye effect is expected when an actual, three-dimensional person is present, an absence of the relative change in the dimensions of the facial features alerts the system to a fraudulent attempt at authentication. This effect could not easily be re-created with a two dimensional picture (printed photograph or screen) and thus, this step can serve as a secure test to prevent a two dimensional picture (in place of a live face) from being used for authentication.

[0164] In other words, using this movement of "zooming" in and out on the user's face, two or more biometric profiles could be created for the same person. One of the multiple profiles for the person may be imaged farther from the camera, and one of the multiple profiles may be for the person imaged closer to the camera. In order for the system to authenticate the person, the authentication images and biometrics must match the two or more profiles in the enrollment images and biometrics.

[0165] In addition, the system may detect the presence of a real person as compared with a fraudulent photograph of a person by comparing the background of the images obtained at a close and a far proximity. When the mobile device 1310 is held such that the person's face fits within the oval 1320, objects in the background that are almost directly behind the

person may be visible. However, when the mobile device 1310 is held such that the person's face fits within the larger oval 1330, the person's face blocks the cameras ability to see the same objects that are almost directly behind the person. Thus, the system may compare the backgrounds of the images obtained at the close and the far proximity to determine whether the real person is attempting authentication with the system.

[0166] Of course, in Figures. 13A and 13B, shapes or guides other than ovals 1320 and 1330 may be used to guide the user to hold the mobile device 1310 at the appropriate distance from his or her face. For example, the mobile device 1310 may show a full or partial square or rectangle frame. Further, the system may vary the size and location of the frame, such as the ovals 1320, 1330 to add further security. For example, the system may require a medium sized frame, a small frame, and then a large frame. As another example, the system may require a small frame at a first location and a second location, and then a large frame. This may be done randomly in order to teach different users different enrollment and authentication movements.

[0167] The number of frame sizes presented to the user may also vary for a single user based on the results of other security features described herein. For example, if the GPS coordinates of the mobile device show that the device is in an unexpected location, more frames at different distances may be required for authentication. One or more indicators, such as lights, words, or symbols may be presented on the screen so as to be visible to the user to direct the user to the desired distance that the mobile device should be from the user.

[0168] In Figures 13A and 13B, the system may predict the expected fish-eye distortion of the images based on the mobile device used for enrollment and authentication, and based on known and trusted enrollment data. In addition or as an alternative, the known specifications of a mobile phone camera for a given model may be utilized to predict the expected distortion of the person's facial features at different distances from the lens. Thus, the authentication may be device dependent. Further, enrollment information from the user is not required at every possible distance from the camera.

[0169] For example, as described above, enrollment images and biometrics may be obtained for a user at two distances from the user. During authentication, multiple images are captured in addition to images corresponding the close and far distances of the enrollment images and biometrics. Based on the expected distortion of these intermediary images according to the distanced traveled by the device, the system may validate that the change in distortion of the images is happening at the correct rate, even though only two enrollment profiles are obtained.

[0170] The capturing of these images may be still images or video, such that frames or images are extracted from the video that is taken during the movement from the first position distant from the user and the second position proximate the user. Thus, it is contemplated the operation may capture numerous frames during the zoom motion and ensure that the distortion is happening at the correct rate for the head size and the movement of the mobile device distance based on data from the accelerometers, magnetometers, and so forth.

[0171] Over time based on accumulated data, or calculated data during design phase, the system will have data indicating that if a phone is moved a certain distance toward a user's face, then the distortion effect should fall within a known percentage of the final distortion level or initial distortion level. Thus, to fool or deceive the authentication system disclosed herein, the fraud attempt would not only need to distort the fraudulent two-dimensional picture image, but would also need to cut the background, and then make a video of the face, distortion, and background that does all of this incrementally and at the correct speed, all while not having any banding from the video screen or having any screen edges visible, which is very unlikely.

[0172] Many currently known facial detection and facial recognition algorithms are configured to look for a small face within an image. Thus, in order to ensure that the facial detection and recognition algorithms detect and recognize the user's face in the zoomed in image (Figure 13B), the system may add a large buffer zone around the image taken at a close proximity. This creates a larger overall image and allows current facial detection and recognition algorithms to detect and recognize the face, even where the face of the user is large in the original image.

[0173] When the enrollment and authentication movement resulting from the process described with Figures 13A and 13B is used, the eye tracking security features described above may also be enhanced. For example, when the user is instructed to bring the mobile device 1310 closer to his or her face to fill the oval 1330, the QR code, a random shape, a bar code, color, text, numbers or any other visual indictor may be displayed on the screen.

At this close distance, the reflection of the displayed indicator off of the user's eye or face may be more easily imaged by the camera. Furthermore, eye movement, blinking, and the like to determine the "liveness" of the person being imaged may also be more easily obtained at the close proximity.

[0174] In one embodiment, at least one blink is required to prove liveness for authentication. In another embodiment, blinks may be counted and the number of blinks may be averaged over time during authentications. This allows for an additional factor in authentication to be the number of blinks observed during the motion. If a pattern of when the user blinks during the motion is observed, the system may verify that the user blinks at the expected time and device location during the motion during future authentication attempts.

[0175] In other embodiments, the size or location of the oval or frame may change to sizes or locations other than that shown in Figures 13A, 13B such that the user must position and/or angle the phone to place his or her face within the oval. This establishes yet another method of insuring liveness of the user.

[0176] In one exemplary method, the mobile device is positioned at a first distance from the user and a first image captured for processing. This distance may be linearly away from the user and in this embodiment not in an arc or orbit. This may occur by the user moving the mobile device, either by hand, or by the mobile device being on a movable device or rail system. Or, the lens system may be adjusted if in a fixed system to change

the size of the user's face in relation to the frame size. Alternatively, the user may stay stationary, the multiple cameras may be used, or camera may move without the user moving. Once some form of movement (from a device, camera, lens, or user) has occurred to establish the camera at a second distance, a second image is captured for processing. Movement from the first position to the second position may be straight toward the user. Processing occurs on both images.

[0177] The processing may include calculations to verify a difference between the two images, or a difference in biometrics obtained from the two images, that indicates that a real person is being imaged. Processing may occur to compare the first authentication image to a first enrollment image (corresponding to the first distance) to determine if a match is present and then compare the second authentication image to a second enrollment image (corresponding to the second distance) to determine if a match is present. If a match occurs, then authentication may proceed.

[0178] Variations on these methods are also possible with the system requiring a match at the first distance, but a failure to match at the second distance, thereby indicating that the second image is not of a two-dimensional picture. The processing resulting in a match or failure to match may be any type image or facial recognition processing algorithm. As with other processing described herein, the processing may occur on the mobile device, one or more remote servers, or any combination of such devices.

[0179] All the processing described herein may occur on only the mobile device, only a remote server, or a combination there. The biometric data may be stored on the mobile device or the server, or split between the two for security purposes. For example the images could be processed on the mobile device, but compared to enrollment data in the cloud or at a remote server. Or, the images could be sent to the cloud (remote server) for processing and comparison.

Touch Screen Enhancements

[0180] Additional added security modifications may include information about a user's finger. Many mobile devices with touch screens can detect the location and approximate size of a user's touch on the screen. Accordingly, an approximate size of a user's finger or thumb may be measured by the system. In addition to the size of a finger, an orientation angle of the finger or whether the fingers or thumbs of the right or left hand are used can be detected.

[0181] In one embodiment, a user selects an account to open, begins enrollment imaging, or begins authentication imaging by touching the touchscreen of the user device. The authentication system may thus detect whether the touch by a user during authentication corresponds with previously stored enrollment information including the size of the user's finger or thumb, amount of pressure applied to the screen and whether the user is right or left handed. This adds an additional security layer for the authentication system.

[0182] Furthermore, the authentication system may require that the user initiates an authentication by touching a fingerprint reader or the touchscreen in one or more predetermined manners. In one embodiment, as shown in Figure 14, a touchscreen 1410 may be divided up into predetermined regions 1420. For example, there may be nine equal, circular, square, or other shaped regions 1420 on the touchscreen 1410 of the mobile device. During enrollment, the user selects one of the regions 1420 of the screen 1410 to touch to initiate authentication. During authentication, if the preselected region 1420 is not touched to begin authentication or during the entire authentication process, then authentication is denied. This is but one possible design possibility and other design options are contemplated.

[0183] The regions 1420 on the touchscreen may be visually represented by a grid, or may not be displayed at all on the touchscreen 1410. As shown in Figure 15, in addition to or in place of the regions 1420, buttons 1520 may be displayed on a touchscreen 1510. Here, the user may initiate the authentication by pressing one or more of the buttons 1520 in a predetermined pattern. The user may also initiate authentication via a predetermined swiped pattern. The position to be touched by the user may change with each authentication attempt and may be conveyed to the user through any instructions from the authentication server, such as a code, number, letter, color, captcha or other indicator.

Voice Parameters

[0184] It is also contemplated that the user could record their voice by speaking a phrase while recording their images during the enrollment process when first using the system. Then, to authenticate, the user would also have to also speak the phrase when also moving the mobile device to capture the image of their face. Thus, one additional path parameter may be the user's spoken voice and use of voice recognition as another layer or element of the authentication process.

Image Quality Assurance

[0185] The authentication system may also process the images received from the mobile device to determine if the images are of sufficient quality. For example, the system may check the images for blurriness caused by the images being out of focus or by the camera lens being obscured by fingerprints, oils, etc. The system may alert that user that the quality of the images is insufficient (or too bright or too dark) and direct the user to adjust a focus, exposure, or other parameter, or to clean the lens of the camera.

Autofocus

[0186] The authentication system may also utilize an autofocus feature when the mobile device camera is equipped with such. For example, when an actual, three-dimensional person is being imaged, the system checks to ensure that the sharpness of the image changes throughout as the camera perform auto-focusing. In another embodiment, the system may control the autofocus so that the camera focuses on a first location or distance to check for

sharpness (in focus) of a portion of the image containing a face. The system then controls the camera to focus at a second location or distance where the presence of a face is not detected and check for sharpness (in focus) of a portion of the image. If a three dimensional person in a real environment is being imaged, it is expected that the focal length settings should be different at the first and second locations, which suggests a real person is presently being imaged. However, if the focal lengths of both locations are the same, this indicates that a two dimensional photograph or screen is being imaged, indicating a fraudulent login attempt.

[0187] The system may also control the auto-focus of the device to check for different focal lengths of different particular features in the image. For example, when a person's face is imaged from the front, a person's ear is expected to have a different focal length (more distant) than the tip of a person's nose.

Images of Login Attempt

[0188] The authentication server may also be configured to store the authentication images for a predetermined length of time. The images may provide additional security benefits as evidence of a person attempting to log in to a user's account. For example, the system may store a predetermined number of prior log in attempts, such as twenty login attempts, or store images from login attempts for a predetermined time period, such as during the past seven days or weeks. Any fraud or attempted fraud will result in pictures of the person attempting the login being stored or sent to the authentication server of the account server.

[0189] The mere knowledge that photos will be taken and sent is a significant deterrent to any potentially dishonest person because they know their picture will be taken and stored, and it is an assurance of security to the user. Likewise, any attempted and failed attempt can have the photo stored and indicator of who is attempting to access the account. It is also contemplated that an email or text message along with the picture of the person attempting the failed log in may be sent to the authorized user so they know who is attempting to access their account. This establishes the first line of security for the account as the user with the photo or image also being possessed by the authentication server.

Adaptive Match Thresholds

[0190] Further, the level or percentage of correspondence between the enrollment information and the authentication information to authenticate the user may change over time. In other words, the system may comprise an adaptive threshold.

[0191] After a user regularly uses the authentication system described above, the user will have logged in with the system by moving the mobile device in the predetermined path relative to his or her head a large number of times. Accordingly, it may be expected that as the user will gain experience using the authentication system, and that the user will gradually settle into a comfortable and standardized motion path. In contrast, the initial

enrollment movement of a user will likely be the most awkward and clumsy movement as the user has little experience with the authentication system.

[0192] In order to make the authentication system more convenient for the user without losing security, the adaptive threshold system allow the enrollment movement to adapt so that the user is not locked into the awkward and clumsy initial movement as the enrollment movement. To facilitate this, upon each successfully authorization, the successful authorization movement is stored, and the motion path is added to a list of acceptable motion paths. The list of acceptable motion paths may be limited to a predetermined number of paths. When a new successfully authorization is completed and the list of acceptable motion paths is full, the older enrollment motion path is deleted and the newest is stored in its place. Alternatively, the motion path that is least similar to the other motion paths stored on the list may be deleted. Thus, by storing the most alike or newest motion paths, the enrollment movement may slowly adapt over time as the user because familiar with the system and settles into a comfortable motion path for authentication.

[0193] In addition, other enrollment information may adaptively change in a similar manner as the user information. For example, successful authentication photos or biometric information can be stored as part of the enrollment information, and old enrollment information may be discarded over time. In this manner, the authentication system can be convenient for a user even over a long period of time as the user experiences aging, facial hair growth, different styles of makeup, new glasses, or other subtle face alterations.

[0194] Determining how much variance is allowed over time in the motion path or the biometric information, or both may be set by the entity requiring authentication in order to meet that entity's security requirements. Time or number of scans after the initial enrollment can be used to modify the adaptive threshold. For example, during a first few days after enrollment, the threshold may be lower while a security threat is low and the differences in paths are likely to be higher. After a number of authentications or a number of days, the threshold may increase. The threshold further may be set based on trending data of either the motion path or biometric information. For example, the threshold may be more lenient in a direction the data is trending, while having a tighter tolerance for data against the trend.

[0195] A temporal aspect may also be added along with the location information. For example, if the user conducts and authenticates a transaction near his home, and then one hour later another transaction is attempted in a foreign country, the transaction may be denied. Or it may be denied if the distance between the prior authentication location and the next authentication location cannot be traveled or is unlikely to have been traveled in the amount of time between login or authentication attempts. For example, if the user authenticates in Denver, but an hour later an attempt is made in New York, Russia or Africa, then either first or second attempt is fraudulent because the user likely cannot travel between these locations in 1 hour.

[0196] Further, if the next transaction is attempted at a more reasonable time and distance away from the first transaction, the level of correspondence threshold may be raised to

provide added security, without automatically denying the transaction. Likewise, an altimeter may be used such that if the altitude determined by the mobile device is different than the altitude of the city in which the user is reported to be located, then this may indicate a fraud attempt. Thus, altitude or barometric readings from the mobile device may be used to verify location and can be cross referenced against GPS data, IP address or router location data, or user identified location.

Random Image Distortion

[0197] In order to provide an additional layer of security to the facial recognition authentication system, the system may utilize random image distortion. For example, a user may be assigned a random distortion algorithm upon enrollment into the system. The distortion algorithm may include such distortions to the image as widening or narrowing the person's face by a predetermined amount, adding or superimposing a predetermined shape at a predetermined position on the user's face. As one example of this, the distortion may be a circle superimposed at 100 pixels above the user's left eye.

[0198] With the uniquely assigned distortion on the images from the user, the biometric data for that user will be unique to the account or device used by the user. That is, the enrollment biometrics stored on the authentication server or on the mobile device will reflect not only the facial features of the user, but also will reflect the uniquely assigned image distortion. Thus, even if an accurate, fraudulent representation of a person were used on a different device or via a different account, the proffered authentication biometrics

would not sufficiently correspond due to a different or an absence of the unique distortion. Thus, the overall security may be enhanced.

Security Layers

[0199] It is noted that each of the above embodiments, modifications, and enhancements may be combined in any combination as necessary to create multiple layers of security for authentication. For example, the facial recognition may be combined with motion detection or path detection, or operate independently of these features for authentication. Further, when more than one of the above described enhancements or modifications are combined, the authentication system may be configured so as not to provide any feedback or indication on which layer failed authentication.

[0200] For example, when a predetermined touch pattern to initiate authentication is combined with the authentication movement and facial authentication, the system does not indicate whether a touch pattern was incorrect, or the authentication movement or authentication images failed to correspond to the enrollment information. Instead, the system provides an identical denial of authentication no matter what failure occurs. This is the case when any number of the security features described above are combined. In this manner, it is difficult for a fraudster to detect what aspect of the fraudulent credentials must be corrected, further enhancing the security of the system.

[0201] All of the above features may be incorporated together, or only some features may be used and others omitted. For example, when the device prompts the user to move the device so that the user places his or her head within a first small frame (such as an oval) then to a second large frame (such as in FIGS. 7A, 7B, 13A, and 13B), the system may be configured such that facial recognition need not be performed on the image(s) in the first frame (distantly captured frames). The security of the system is maintained by performing facial recognition throughout the imaging at some point between the first and second frames, and at the second frame. This may especially be true when also integrated another layer of security, such as checking eye tracking following a moving object on the screen, or reading a reflection of a QR code or random shape off of the user's eye. In another embodiment, when two or more cameras are used creating three dimensional, stereoscopic images, the facial recognition may not be performed at the first, far away frame, but instead the liveness of the person may be validated at the closer in frame only after the movement of the device. In still other embodiments, other security layers may be used, and the motion parameters may be omitted. Such combinations may be beneficial for larger or stationary devices, such as gaming laptop computers, personal desktop computers, a stationary kiosk, or the like.

Example Applications

[0202] Likewise, although described herein as financial account authentication, the authentication using path parameters and image data may be implemented in any environment requiring verification of the user's identity before allowing access, such as

auto access, room access, computer access, web site or data access, phone use, computer use, package receipt, event access, ticketing, courtroom access, airport security, retail sales transaction, IoT access, or any other type of situation.

[0203] For example, an embodiment will be described where the above authentication system is used to securely conduct a retail sales transaction. In this embodiment, a user is enrolled with the authentication server or an authentication application on the mobile device as described above and has generated enrollment information including enrollment images and/or biometrics, and enrollment movement. In this example, the user initiates or attempts to complete a transaction at a retail establishment with a credit card, smart card, or using a smart phone with NFC capabilities.

[0204] The user begins the transaction by swiping a credit card, smart card, or using an application on a smartphone with NFC capabilities to pay for goods or services. The retail establishment would then authorize the card or account with the relevant network of the financial institution ("Gateway"). For example, the retail establishment, through a Gateway such as one operated by VISA or AMERICAN EXPRESS would determine whether the account is available and has sufficient available funds.

[0205] The Gateway would then communicate with the authorization server to authorize the transaction by verifying the identity of the user. For example, the Gateway may send an authorization request to the authentication server, and the authentication server then

sends a notification, such as a push notification, to the user's mobile device to request that the user authenticate the transaction.

[0206] Upon receipt of the notification from the authentication server, such as through a vibration, beep, or other sound on the mobile device, the user may then authenticate his or her identify with the mobile device. The authentication server may also send information concerning the transaction to the user for verification by the user. For example, the authentication server may send information that causes the mobile device to display the merchant, merchant location, and the purchase total for the transaction.

[0207] Next, as before, the user may hold the mobile device and obtain a plurality of authentication images as the user moves the mobile device to different positions relative to the user's head. While moving the mobile device to obtain the authentication images, the mobile phone further tracks the path parameters (authentication movement) of the mobile device via the gyroscope, magnetometer, and the accelerometer to obtain the authentication movement of the device. The mobile device may then send the device information, the authentication images, and the authentication movement to the authentication server. In other embodiments, the mobile device may process the images to obtain biometric data and send the biometric data to the server. In still other embodiments, the mobile device may process the images, obtain the authentication information, compare the authentication information to enrollment information stored on the mobile device, and send pass/fail results of the comparison to the authentication server.

[0208] The authentication server may then authenticate the identity of the user and confirm that the user wishes to authorize the transaction on his or her account if the device information, authentication images and/or biometrics, and authentication movement correspond with the enrollment device information, the enrollment images and/or biometrics, and the enrollment movement. The authentication server then transmits an authorization message to the Gateway. Once the gateway has received confirmation of the authorization, the Gateway then communicates with the retail establishment to allow the retail transaction.

[0209] Several advantages may be obtained when a retail transaction is authorized utilizing the above system and method. Because the identity verification of the user and the confirmation of the transaction is completed via the authentication system and mobile device, there is no longer a requirement for a user to provide his or her credit card or signature, or to enter a pin number into the retailer's point of sale system. Further, the retail establishment does not need to check a photo identification of the user. The above method and system also has the advantage that it provides secure transactions that can work with mobile and online transactions that do not have cameras, such as security cameras, on the premises.

[0210] In the secure retail transaction described above, the user obtains the total amount due on his or her mobile device from the retail establishment via the Gateway and authentication server. However, in one embodiment, the mobile phone may use the camera as a bar code, QR code, or similar scanner to identify the items and the prices of the items

being purchased. The mobile device may then total the amount due and act as the checkout to complete the transaction with the retail establishment.

[0211] In another embodiment, a user of the application may want to anonymously pay an individual or a merchant. In this instance, the user would designate an amount to be paid into an application, and the application would create a unique identifying transaction number. This number may then be shown to the second user, so the second user can type the identifying transaction number on an application on a separate device. The unique identifying transaction number may also be sent from the user to the second user via NFC, Bluetooth, a QR code, or other suitable methods. The second user may also type the amount and request payment.

[0212] Upon receiving the payment request and unique identifying transaction number, the authentication server may send a notification to the first user's mobile device to authenticate the transaction. The user would then verify his or her identity using the facial recognition authentication system described above. The user may alternatively or additionally verify his or her identity using other biometric data such as a fingerprint or retina scan, path based motion and imaging, or the user may enter a password. Upon authentication, the user's device would send a request to the user's payment provider to request and authorize payment to the second user. In this manner, the payment may be done securely while the users in the transaction are anonymous.

[0213] According to one embodiment, as an additional measure of security, the GPS information from the mobile device may also be sent to the authentication server to authenticate and allow the retail transaction. For example, the GPS coordinates from the mobile device may be compared with the coordinates of the retail establishment to confirm that the user is actually present in the retail establishment. In this manner, a criminal that has stolen a credit card and attempts to use the card from a distant location (as compared to the retail location) is unable to complete a transaction because the user's phone is not at the location of the retail establishment. IP addresses may also be used to determine location.

[0214] As explained above, the level or percentage of correspondence between the enrollment information and the authentication information to authenticate the user may also be adjusted based on the coordinates of the GPS of the mobile device. For example, if the retail establishment and GPS coordinates of the mobile device are near a user's home, then the level of correspondence may be set at a lower threshold, such as at a 99% match rate. Alternatively, if the location is very far from the user's home, and is in a foreign country, for example, then the level of correspondence may be set at a higher threshold, such as at a 99.999% match rate.

[0215] While various embodiments of the invention have been described, it will be apparent to those of ordinary skill in the art that many more embodiments and implementations are possible that are within the scope of this invention. In addition, the

various features, elements, and embodiments described herein may be claimed or combined in any combination or arrangement.

CLAIMS

What is claimed is:

1. A method for enrolling and authenticating a user in an authentication system via a user's a mobile computing device comprising a camera and at least one movement detecting sensor, the method comprising:

capturing enrollment biometric information from at least one first image of the user, the first image recorded by the camera of the mobile device;

storing the enrollment biometric information on a memory;

capturing authentication biometric information from at least one second image of the user, the second image recorded by the camera of the mobile device;

recording, during imaging of the at least one second image, path parameter data from the at least one movement detecting sensor, the path parameter data representing an authentication movement of the mobile device;

comparing the authentication biometric information to the stored enrollment biometric information to determine whether the authentication biometric information meets a predetermine similarity threshold as compared to the enrollment biometric information;

comparing the authentication movement of the mobile device to an expected movement of the mobile device to determine whether the authentication movement meets a predetermine similarity threshold as compared to the expected movement; and

when the authentication biometric information sufficiently corresponds with the enrollment biometric information, and when the authentication movement a predetermine similarity threshold as compared to with the expected movement, authenticating the user.

2. The method according to claim 1, further comprising capturing, during imaging of the at least one first image, enrollment path parameters via the at least one movement detecting sensor, the enrollment path parameters indicating an enrollment movement of the mobile device, and defining the expected movement as the enrollment movement.

3. The method according to claim 1, wherein the at least one first image and the at least one second image of the user include an image of the user's face, and the enrollment biometric information and the authentication biometric information comprise facial recognition information.

4. The method according to claim 1, further comprising:

capturing enrollment device information during imaging of the at least one first image;

storing the enrollment device information on the memory;

capturing authentication device information during imaging of the at least on second image; and

comparing the authentication device information with the enrollment device information to determine whether the authentication device information sufficiently corresponds to the enrollment device information.

5. The method according to claim 4, wherein the device information comprises at least one of the following: a device manufacturer, model number, serial number, and mobile network information.

6. The method according to claim 1, wherein at least one movement detecting sensor comprises at least one of the following: an accelerometer, a magnetometer, and a gyroscope.

7. A facial authentication system utilizing a user's mobile device, the mobile device comprising a camera and at least one movement detecting sensor, the authentication system comprising:

an authentication server comprising a processor, a memory, and at least one transceiver configured to transmit data from the authentication server and received data;

one or more memories configured to store one or more databases, the one or more databases configured to store authentication information profiles; and

machine readable instructions that are stored on the memory of the authentication server which when executed by the processor, cause the authentication server to:

receive enrollment biometrics from the mobile device, the enrollment biometrics comprising facial recognition data processed from at least one first image of the user's face obtained via the camera of the mobile device;

store the enrollment biometrics in the one or more databases and associate the enrollment biometric data with the user authentication information profile;

receive authentication biometrics from the mobile device during an authentication attempt by the user, the authentication biometrics comprising facial recognition data processed from at least one second image of the user's face, the image obtained from the camera of the mobile device;

receive authentication movement information from the mobile device, the authentication movement information comprising data regarding movement of the mobile device during imaging of the at least one second image as detected by the at least one movement detecting sensor in the mobile device;

compare the authentication biometrics and the authentication movement information with the enrollment biometrics and expected movement information stored in the database with the user authentication information profile; and

authenticate or not authenticate the user based on a comparison match rate of the authentication biometrics and the authentication movement with the enrollment biometrics and the expected movement.

8. The facial authentication system of claim 7, wherein

the mobile device displays a first prompt on a display screen to instruct the user to position a face of the user within a first display area of the display screen,

the mobile device display a second prompt on the display screen to instruct the user to position the face of the user within a second display area of the display screen, the second display area being a different size than the first display area, and

the expected movement is based on an anticipated path of the mobile device to place the face sequentially in the first display area and the second display area.

9. The facial authentication system of claim 7, wherein the authentication server detects the presence or absence of banding in the at least one second image.

10. The facial authentication system of claim 7, wherein the authentication server detect the present or absence of a screen edge in the at least one second image.

11. The facial authentication system of claim 7, wherein

the authentication server or mobile device estimates at least one of a gender, age, and ethnicity of a face imaged in the at least one first image,

the authentication server estimates at least one of a gender, age, and ethnicity of the face imaged in the at least one second image, and

the authentication server authenticates or does not authenticate the user based on a comparison match rate of at least one of a gender, age, and ethnicity detected in the at least one first image and the at least one second image in relation to a comparison match rate threshold.

12. The facial authentication system of claim 7, wherein the comparison match rate threshold required for authentication is variable.

13. The facial authentication system of claim 12, wherein the comparison match rate threshold increases based on a number of successful authentications.

14. The facial authentication system of claim 12, wherein the comparison match rate threshold increases over time.

15. A method for authenticating a user in an authentication system via a user's camera equipped computing device, the method comprising:

capturing at least one first image of the user taken with the camera of the computing device at a first distance from the user;

processing the at least one first image to obtain first biometric data based on facial recognition data from the at least one first image;

capture at least one second image of the user taken with the camera of the computing device at a second distance from the user, the second distance being different from the first distance;

processing the at least one second image to obtain second biometric data based on facial recognition data from the at least on second image;

comparing the first biometric data to the second biometric data;

when the first biometric data does not match the second biometric data within a predetermined threshold, authenticating the user; and

when the first biometric data matches the second biometric data within a predetermined threshold, denying access to the user.

16. The method according to claim 15, further comprising:

capturing at least one first enrollment image of the user taken with the camera of the computing device at the first distance from the user;

processing the at least one first enrollment image to obtain first enrollment biometric data based on facial recognition data from the at least one first enrollment image;

comparing the first biometric data to the first enrollment biometric data; and

authenticating the user when the first biometric data matches the first enrollment biometric data within a predetermined threshold.

17. The method according to claim 16, further comprising:

capturing at least one second enrollment image of the user taken with the camera of the computing device at the second distance from the user;

processing the at least one second enrollment image to obtain second enrollment biometric data based on facial recognition data from the at least one second enrollment image;

comparing the second biometric data to the second enrollment biometric data; and

authenticating the user when the second biometric data matches the second enrollment biometric data within a predetermined threshold.

18. The method according to claim 15, wherein the mobile device provides real time video feedback on a display of the mobile device during imaging.

19. The method according to claim 15, further comprising distorting the at least one first image and the at least one second image prior to processing the at least one first image and the at least one second image.

20. The method according to claim 15, further comprising displaying a pattern on the display of the mobile device during the imaging; and

processing the at least one first image or the at least one second image to detect a reflection of the pattern off of an eye or face of the user.

21. The method according to claim 20, wherein the pattern is a unique one-dimensional or two-dimensional barcode.

ABSTRACT

Systems and methods for enrolling and authenticating a user in an authentication system via a user's camera of camera equipped mobile device include capturing and storing enrollment biometric information from at least one first image of the user taken via the camera of the mobile device, capturing authentication biometric information from at least one second image of the user, capturing, during imaging of the at least one second image, path parameters via at least one movement detecting sensor indicating an authentication movement of the mobile device, comparing the authentication biometric information to the stored enrollment biometric information, and comparing the authentication movement of the mobile device to an expected movement of the mobile device to determine whether the authentication movement sufficiently corresponds to the expected movement.

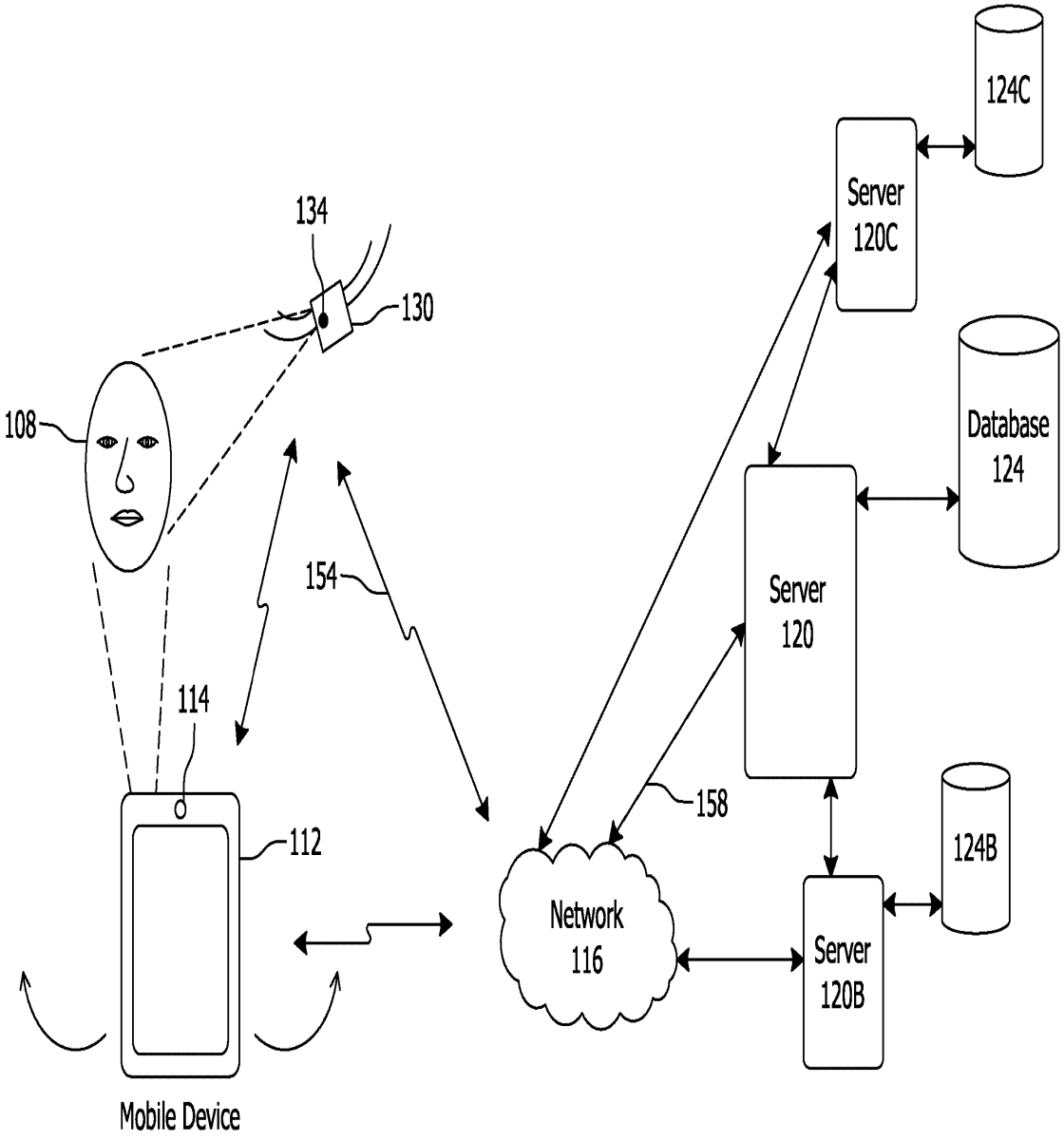

124C
Server
120C
134
130
108
Database
124
154
Server
120
114
158
124B
112
Network
116
Server
120B
Mobile Device

FIG. 1

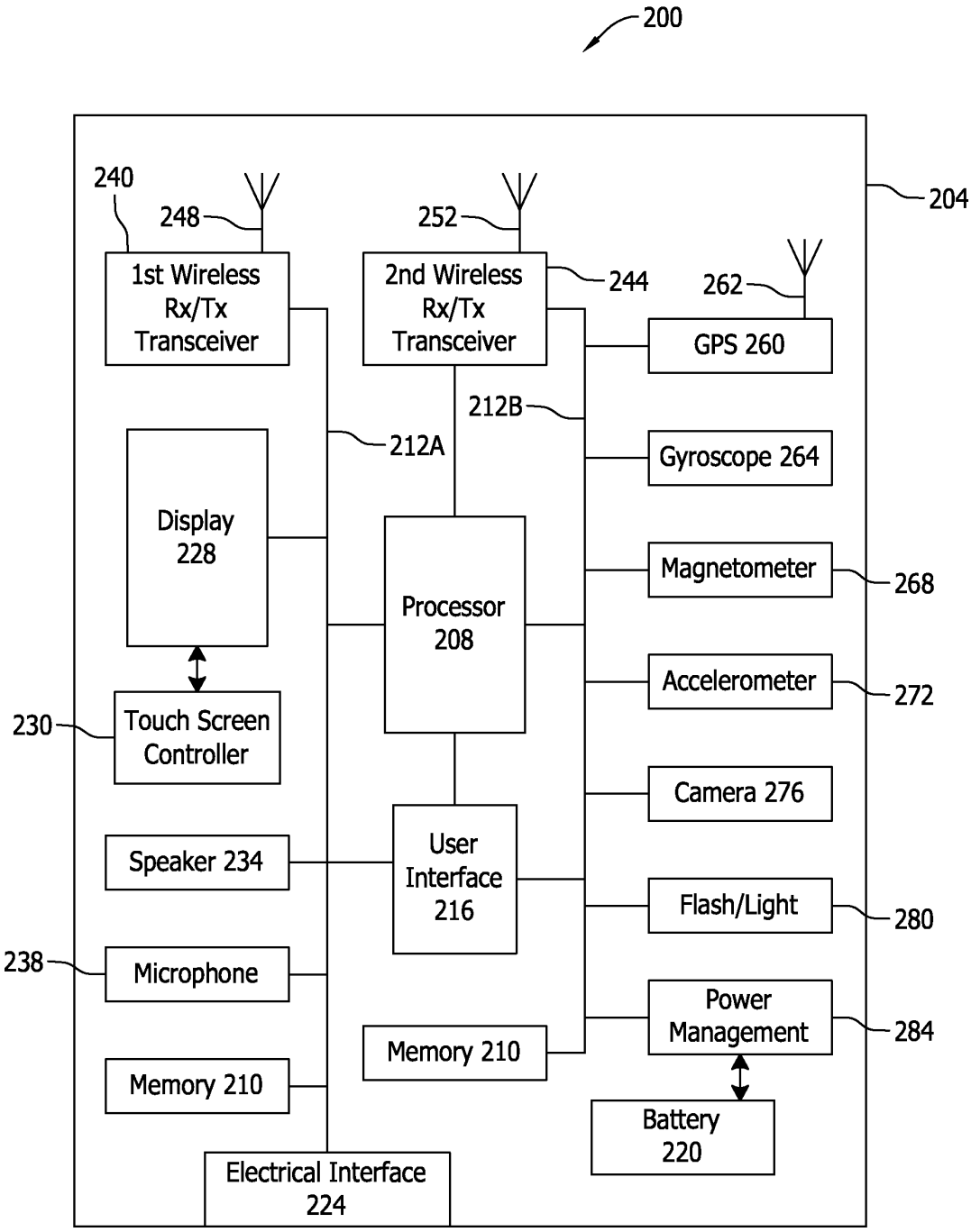

200
204
240
248
252
1st Wireless Rx/Tx Transceiver
2nd Wireless Rx/Tx Transceiver
244
262
GPS 260
212B
212A
Gyroscope 264
Display 228
Processor 208
Magnetometer
268
Accelerometer
272
230
Touch Screen Controller
Camera 276
Speaker 234
User Interface 216
Flash/Light
280
238
Microphone
Power Management
284
Memory 210
Memory 210
Battery 220
Electrical Interface 224

FIG. 2

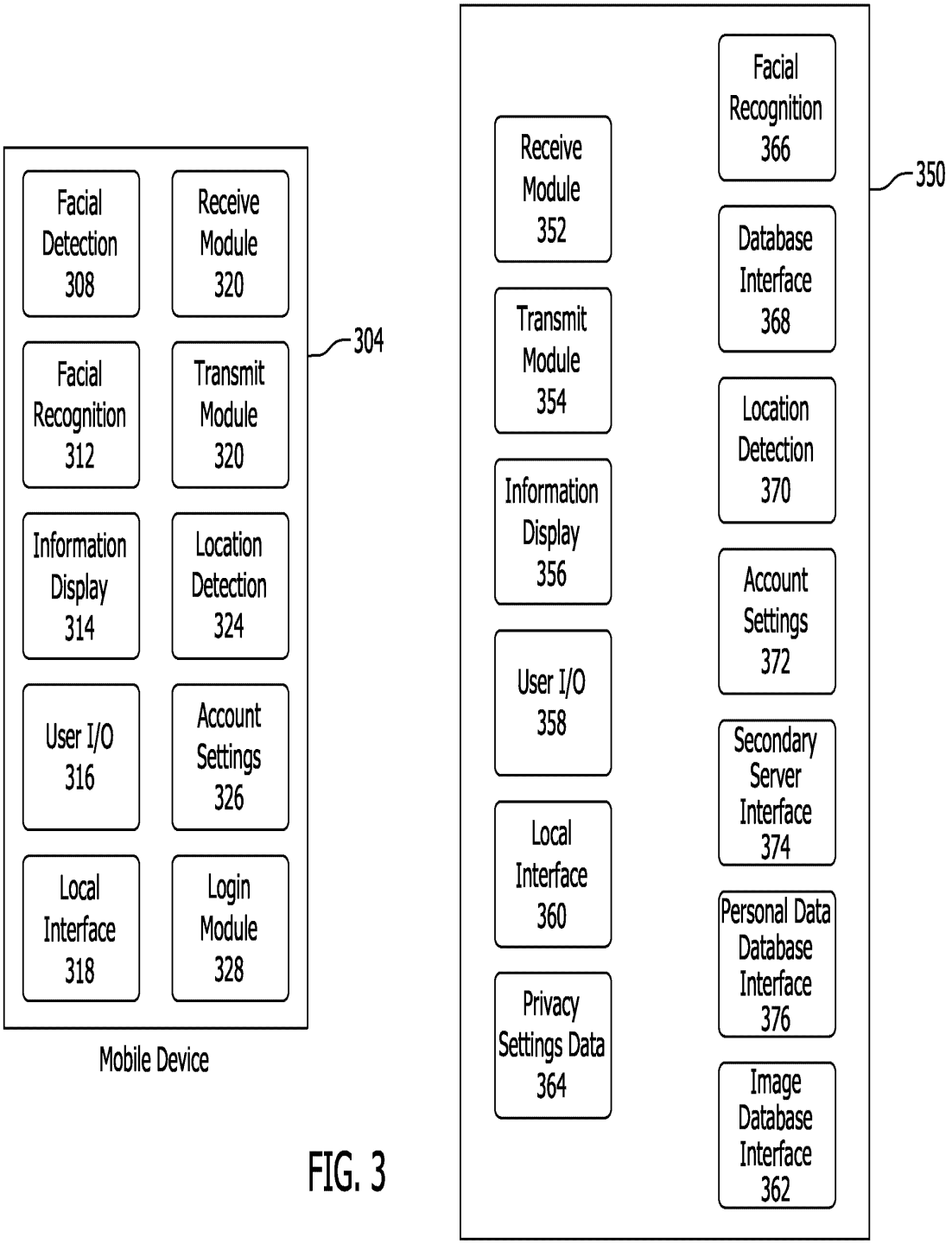

Facial Detection 308
Receive Module 320
Facial Recognition 312
Transmit Module 320
Information Display 314
Location Detection 324
User I/O 316
Account Settings 326
Local Interface 318
Login Module 328
304
Mobile Device
Receive Module 352
Transmit Module 354
Information Display 356
User I/O 358
Local Interface 360
Privacy Settings Data 364
Facial Recognition 366
Database Interface 368
Location Detection 370
Account Settings 372
Secondary Server Interface 374
Personal Data Database Interface 376
Image Database Interface 362
350

FIG. 3

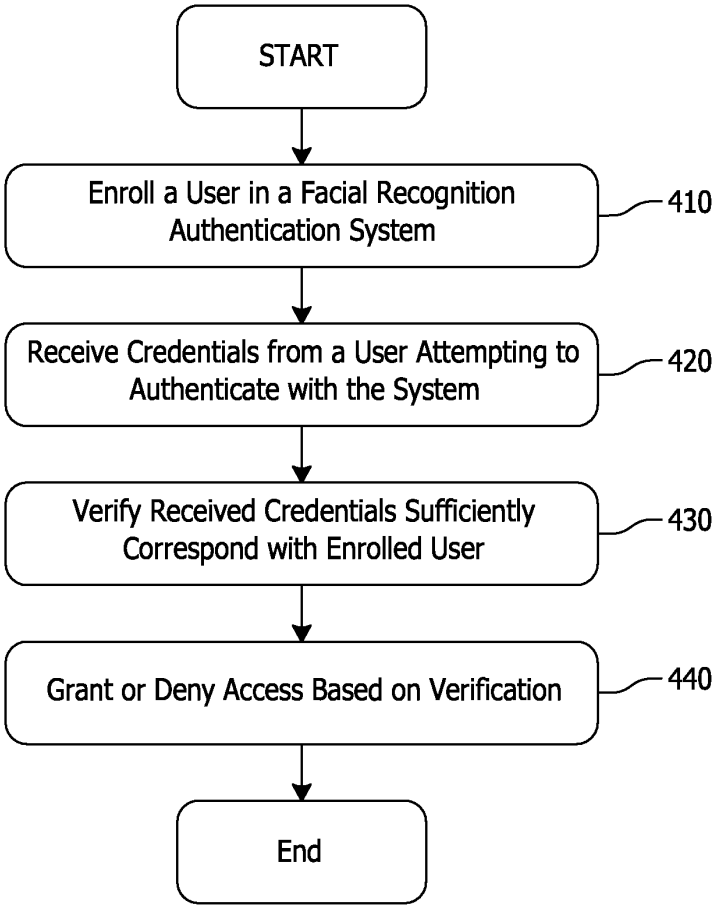

START
Enroll a User in a Facial Recognition Authentication System
410
Receive Credentials from a User Attempting to Authenticate with the System
420
Verify Received Credentials Sufficiently Correspond with Enrolled User
430
Grant or Deny Access Based on Verification
440
End

FIG. 4

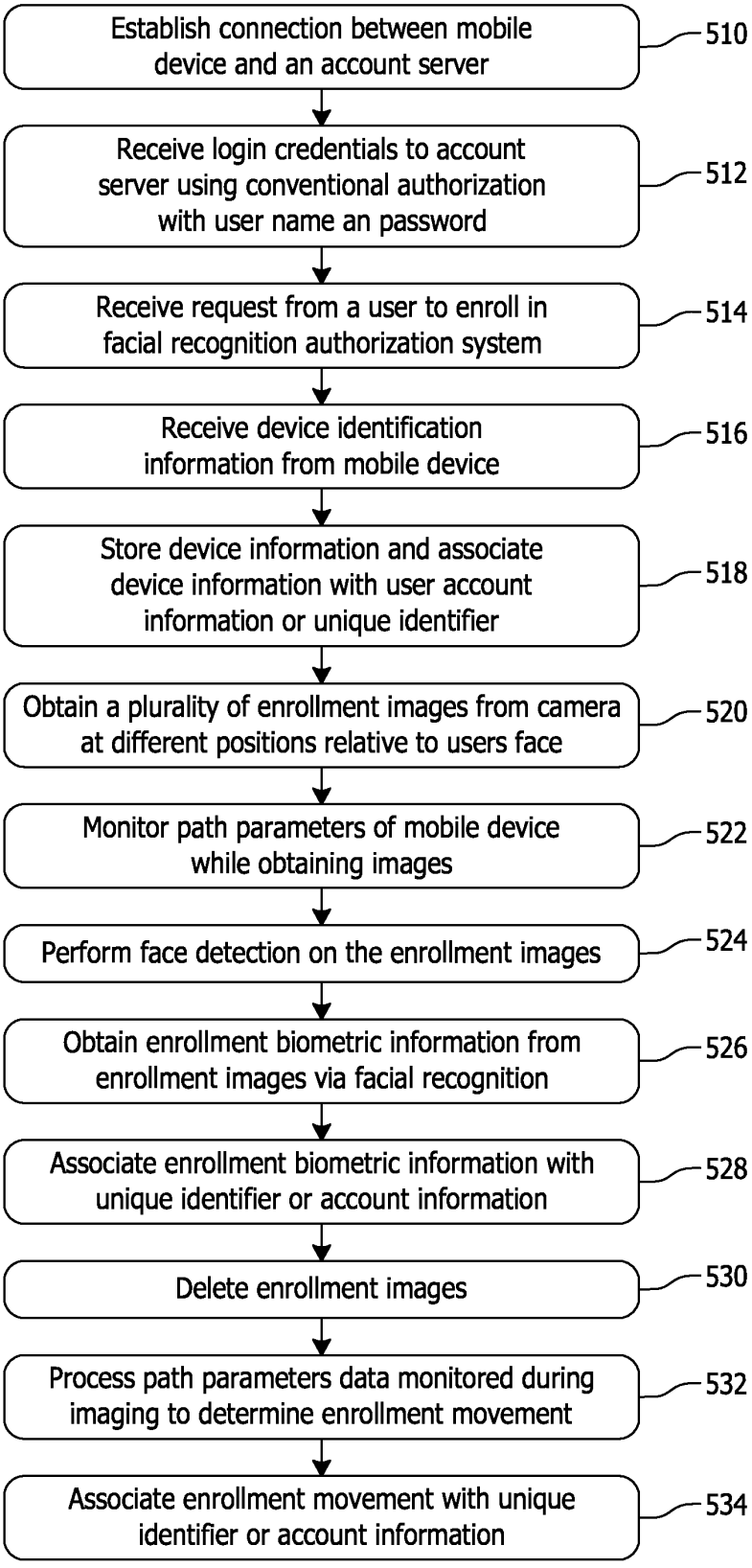

Establish connection between mobile device and an account server
510
Receive login credentials to account server using conventional authorization with user name an password
512
Receive request from a user to enroll in facial recognition authorization system
514
Receive device identification information from mobile device
516
Store device information and associate device information with user account information or unique identifier
518
Obtain a plurality of enrollment images from camera at different positions relative to users face
520
Monitor path parameters of mobile device while obtaining images
522
Perform face detection on the enrollment images
524
Obtain enrollment biometric information from enrollment images via facial recognition
526
Associate enrollment biometric information with unique identifier or account information
528
Delete enrollment images
530
Process path parameters data monitored during imaging to determine enrollment movement
532
Associate enrollment movement with unique identifier or account information
534

FIG. 5

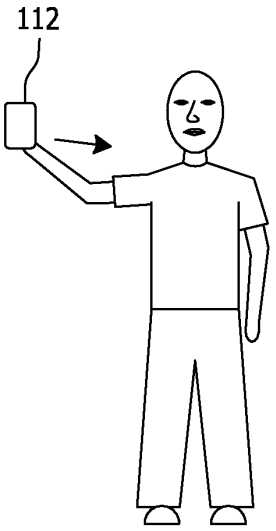


FIG. 6A

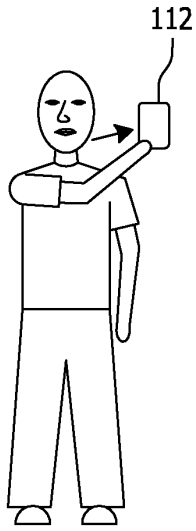


FIG. 6B

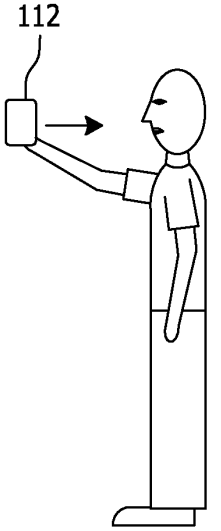


FIG. 7A

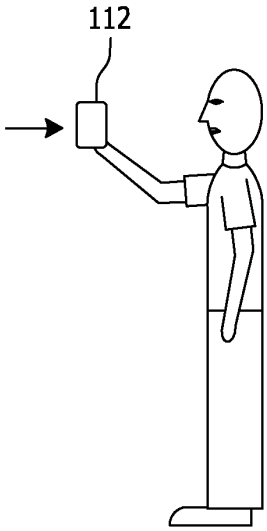


FIG. 7B

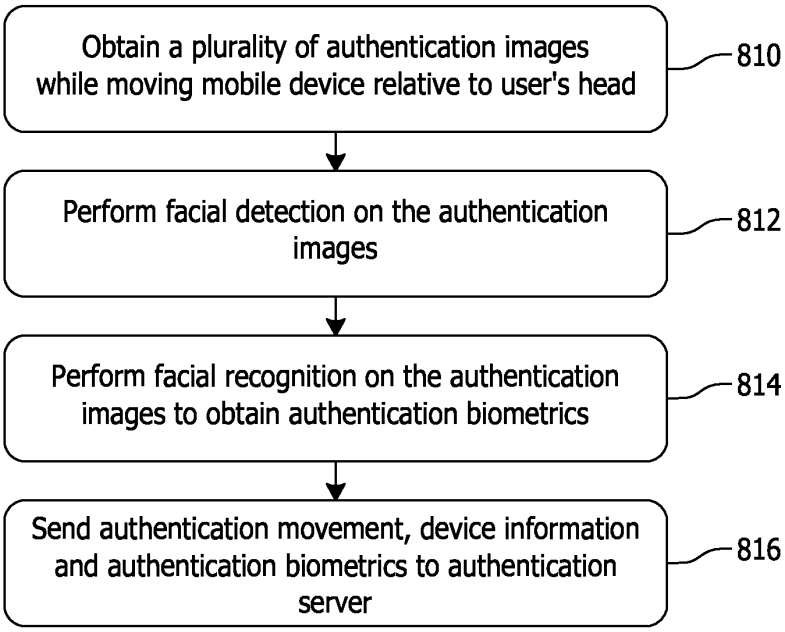

Obtain a plurality of authentication images while moving mobile device relative to user's head
810
Perform facial detection on the authentication images
812
Perform facial recognition on the authentication images to obtain authentication biometrics
814
Send authentication movement, device information and authentication biometrics to authentication server
816

FIG. 8

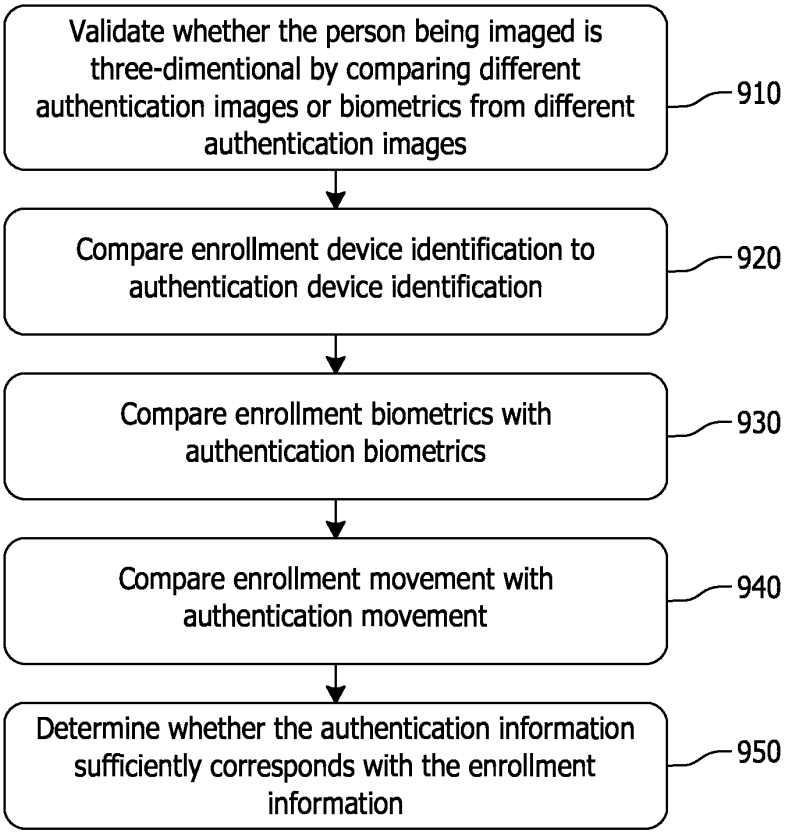

Validate whether the person being imaged is three-dimentional by comparing different authentication images or biometrics from different authentication images
910
Compare enrollment device identification to authentication device identification
920
Compare enrollment biometrics with authentication biometrics
930
Compare enrollment movement with authentication movement
940
Determine whether the authentication information sufficiently corresponds with the enrollment information
950

FIG. 9

FIG. 10

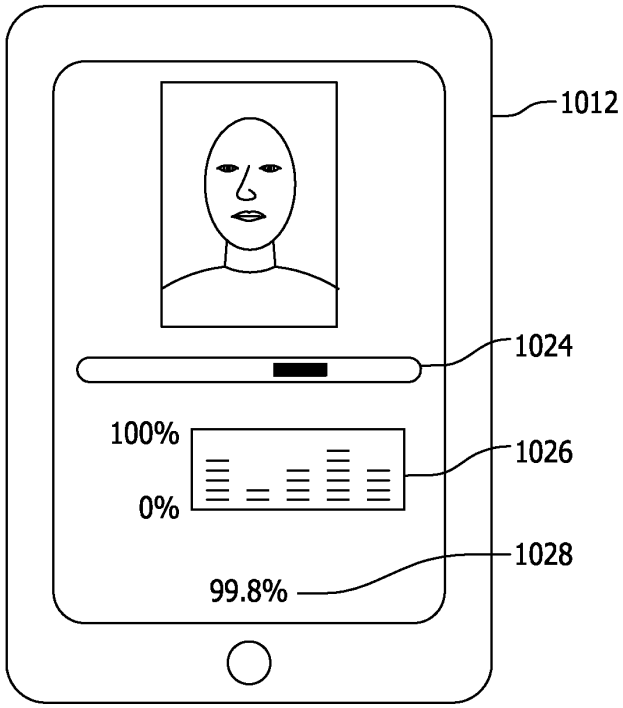
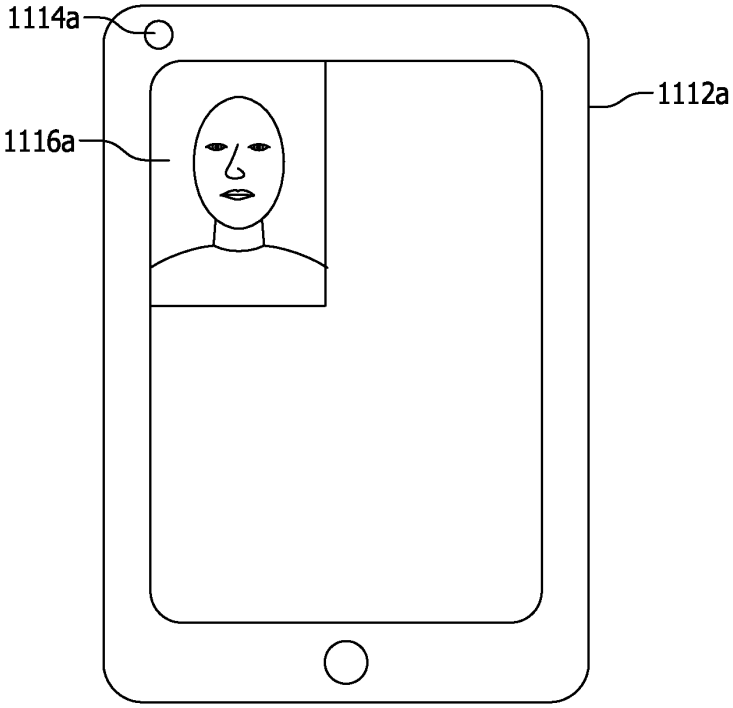


FIG. 11A



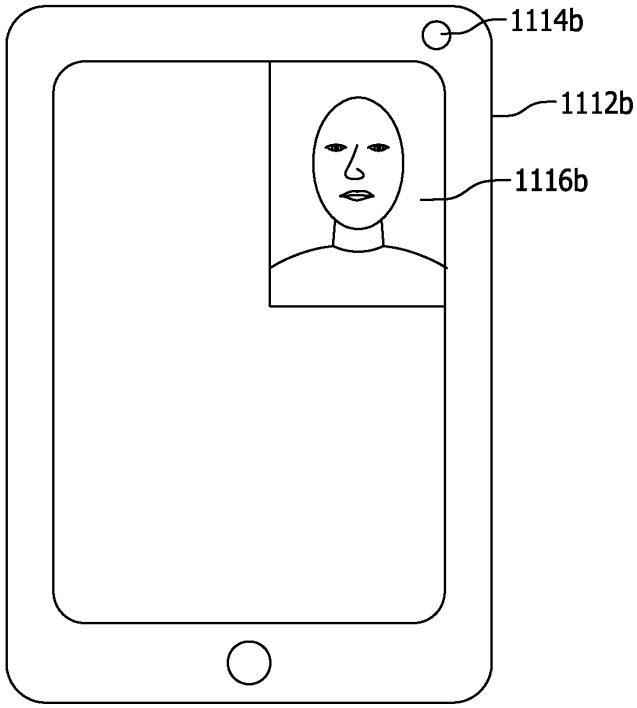


FIG. 11B

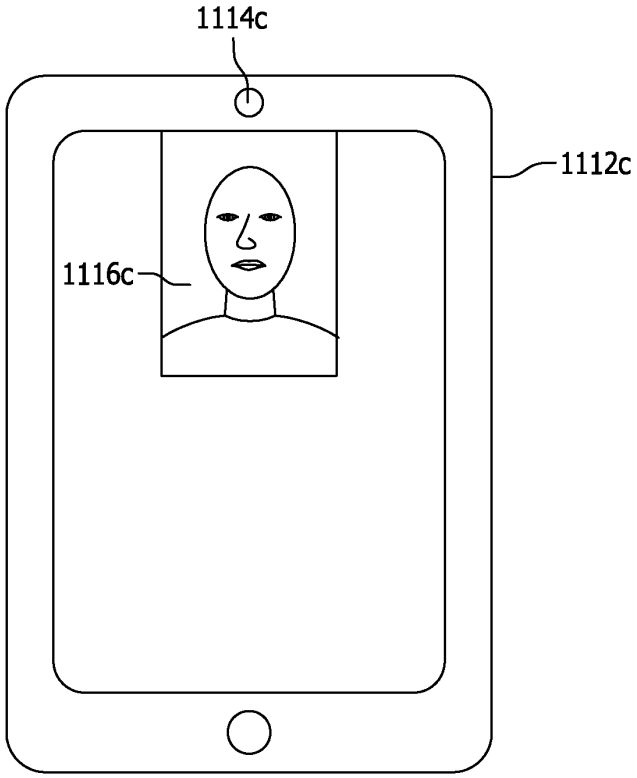


FIG. 11C

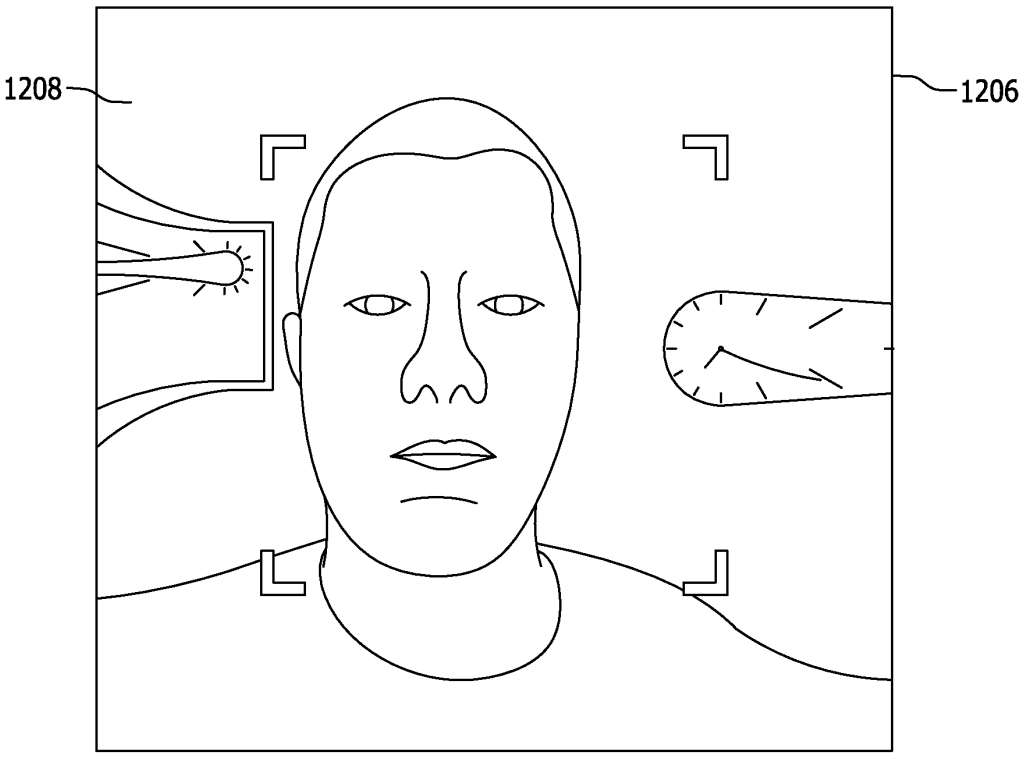


FIG. 12

FIG. 13A

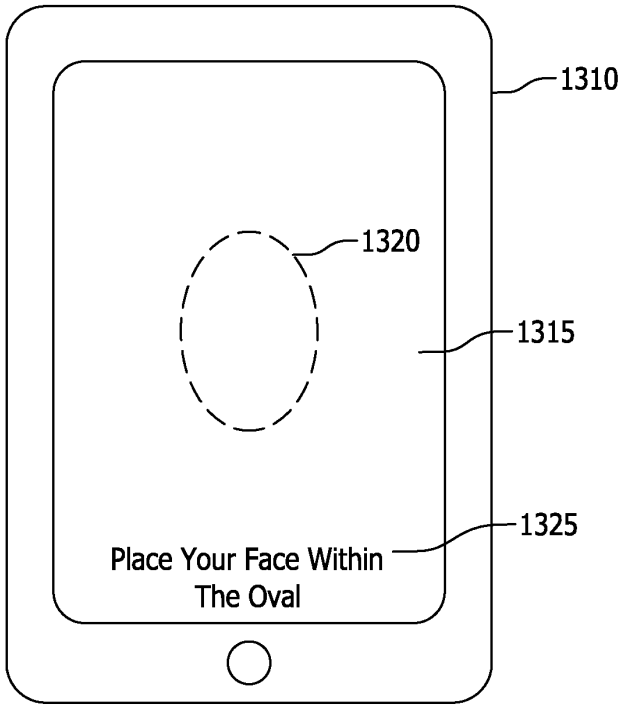
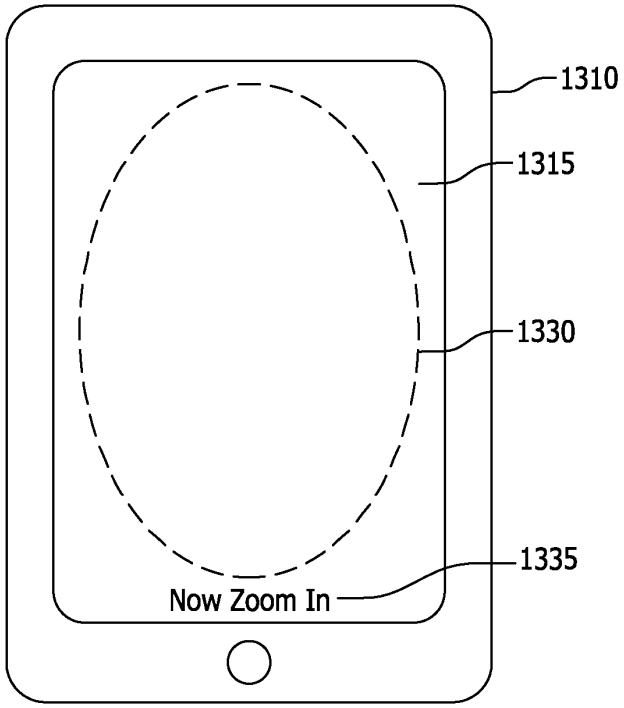


FIG. 13B



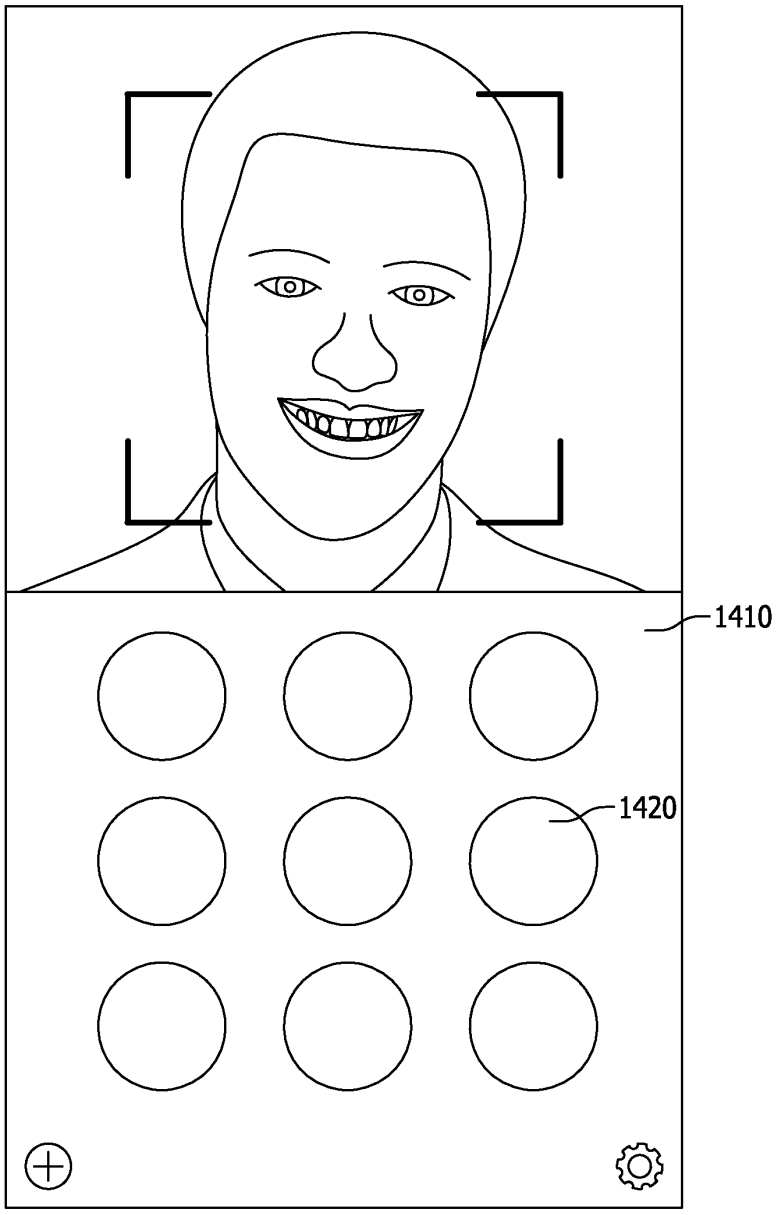


FIG. 14

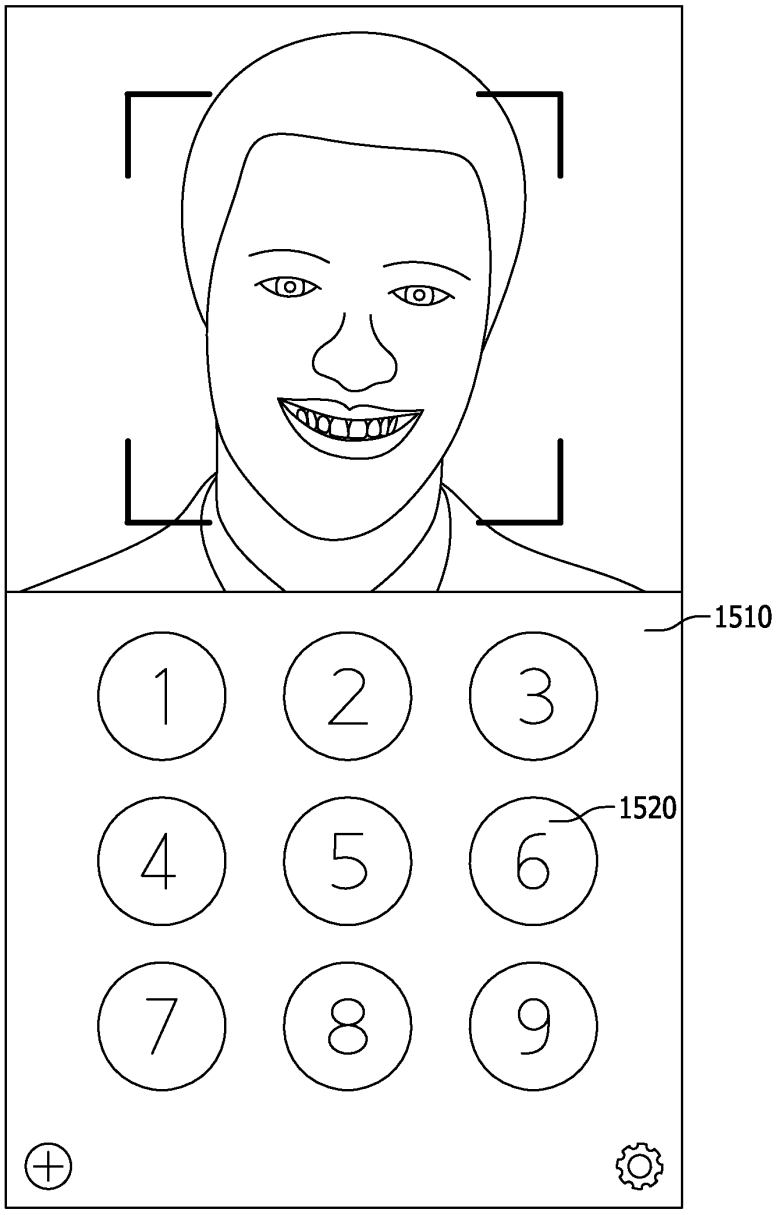


FIG. 15

Electronic Patent Application Fee Transmittal	
Application Number:	
Filing Date:	
Title of Invention:	Facial Recognition Authentication System Including Path Parameters
First Named Inventor/Applicant Name:	KEVIN ALAN TUSSY
Filer:	Brian G. Prince
Attorney Docket Number:	FACIAL.0012P
Filed as Small Entity	
Filing Fees for Utility under 35 USC 111(a)	

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	70	70
Utility Search Fee	2111	1	300	300
Utility Examination Fee	2311	1	360	360
Pages:				
Claims:				
Claims in excess of 20	2202	1	40	40
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	770

Electronic Acknowledgement Receipt	
EFS ID:	23347491
Application Number:	14839505
International Application Number:	
Confirmation Number:	6236
Title of Invention:	Facial Recognition Authentication System Including Path Parameters
First Named Inventor/Applicant Name:	KEVIN ALAN TUSSY
Customer Number:	32856
Filer:	Brian G. Prince
Filer Authorized By:	
Attorney Docket Number:	FACIAL.0012P
Receipt Date:	28-AUG-2015
Filing Date:	
Time Stamp:	17:40:26
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$770
RAM confirmation Number	4290
Deposit Account	502200
Authorized User	PRINCE, BRIAN G.
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	FACIAL0012PADS.pdf	1347507 f3978dd4f435067950d0faaf04f8853f05ffe889	no	7
Warnings:					
Information:					
2	Oath or Declaration filed	FACIAL0012PDECBYINV.pdf	115950 a55d382483bcb94238a95cba25e50f78323d570f	no	1
Warnings:					
Information:					
3		BGPW0428V2SPEC.pdf	363149 bae01d78715c26044aa46107b5bc3880f60ab82e	yes	97

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	87
Claims	88	96
Abstract	97	97

Warnings:					
Information:					
4	Drawings-only black and white line drawings	FACIAL0012PFIGFINAL.pdf	569026 5524248b824f948af3a97b37e091b97313d9da76	no	14
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	36308 fdf323819ec4dd6af5570dbac9950160249c38f6	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2431940		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.